53-1002437-01
January 2012

ServerIron ADX

Global Server Load Balancing Guide

Supporting Brocade ServerIron ADX version 12.4.00

BROCADE

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
ServerIron ADX Global Server Load Balancing Guide	*53-1002437-01*	New document	January 2012

Contents

About This Document

Chapter 1 Global Server Load Balancing

Chapter 2 **Global Server Load Balancing for IPv6**

Appendix A Reference Materials

About This Document

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing.

If you are using a Brocade Layer 3 Switch, you should be familiar with the following protocols if applicable to your network – IP, RIP, OSPF, BGP, ISIS, IGMP, PIM, DVMRP, and VRRP.

Supported hardware and software

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for 12.3.00 documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of this guide:

- ServerIron ADX 1000
- ServerIron ADX 4000
- ServerIron ADX 8000
- ServerIron ADX 10K

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names
	Identifies the names of user-manipulated GUI elements
	Identifies keywords
	Identifies text to enter at the GUI or CLI
italic text	Provides emphasis
	Identifies variables
	Identifies document titles
`code` text	Identifies CLI output

For readability, command names in the narrative portions of this guide are presented in bold: for example, **show version**.

Notes, cautions, and danger notices

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Sun Microsystems	Solaris

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Windows NT, Windows 2000
The Open Group	Linux

Related publications

The following Brocade documents supplement the information in this guide:

- *Release Notes for ServerIron Switch and Router Software TrafficWorks 12.2.00*
- *ServerIron ADX Graphical User Interface*
- *ServerIron ADX Server Load Balancing Guide*
- *ServerIron ADX Advanced Server Load Balancing Guide*
- *ServerIron ADX Global Server Load Balancing Guide*
- *ServerIron ADX Security Guide*
- *ServerIron ADX Administration Guide*
- *ServerIron ADX Switch and Router Guide*
- *ServerIron ADX Firewall Load Balancing Guide*
- *ServerIron ADX Hardware Installation Guide*
- *IronWare MIB Reference*

Getting technical help or reporting errors

Brocade is committed to ensuring that your investment in our products remains cost-effective. If you need assistance, or find errors in the manuals, contact Brocade using one of the following options:

Web access

The Knowledge Portal (KP) contains the latest version of this guide and other user guides for the product. You can also report errors on the KP.

Log in to my.Brocade.com, click the **Product Documentation** tab, then click on the link to the Knowledge Portal (KP). Then click on **Cases** > **Create a New Ticket** to report an error. Make sure you specify the document title in the ticket description.

E-mail and telephone access

Go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

Chapter

Global Server Load Balancing 1

Global Server Load Balancing overview

Global Server Load Balancing (GSLB) enables a ServerIron ADX to add intelligence to authoritative Domain Name System (DNS) servers by serving as a proxy to these servers and providing optimal IP addresses to the querying clients. As a DNS proxy, the GSLB ServerIron ADX evaluates the IP addresses in the DNS replies from the authoritative DNS server for which the ServerIron ADX is a proxy and places the “best” host address for the client at the top of the DNS response.

NOTE
The server no-remote-l3-check command disables Layer3 health checks of IPs learned through GSLB.

NOTE
You need to increase max virtual servers to 1024, max real servers to 2048 and max ports to 4096 to use the max hosts/zone feature.

Do not increase following when use max zone/host feature, or you will run out of memory.

```
system-max ip-static-arp 4096
system-max l3-vlan 4095
system-max mac 64000
system-max ip-route 400000
system-max ip-static-route 4096
system-max vlan 4095
system-max spanning-tree 128
system-max session-limit 1000000
system-max virtual-interface 4095
```

GSLB provides the following advantages:

- No connection delay
- Client geographic awareness based on DNS request origination
- Distributed site performance awareness
- Fair site selection
- Statistical site performance measurements that minimize impact of traffic spikes
- Best performing sites get fair proportion of traffic but are not overwhelmed
- Protection against "best" site failure
- Straight-forward configuration
- All IP protocols are supported

In standard DNS, when a client wants to connect to a host and has the host name but not the IP address, the client can send a lookup request to its local DNS server. The DNS server checks its local database and, if the database contains an Address record for the requested host name, the DNS server sends the IP address for the host name back to the client. The client can then access the host.

If the local DNS server does not have an address record for the requested server, the local DNS server makes a recursive query. When a request reaches an authoritative DNS server, that DNS server responds to this DNS query. The client’s local DNS server then sends the reply to the client. The client now can access the requested host.

With the introduction of redundant servers, a domain name can reside at multiple sites, with different IP addresses. When this is the case, the authoritative DNS server for the domain sends multiple IP addresses in its replies to DNS queries. To provide rudimentary load sharing for the IP addresses for domains, many DNS servers use a simple round robin algorithm to rotate the list of addresses in a given domain for each DNS query. Thus, the address that was first in the list in the last reply sent by the DNS server is the last in the list in the next reply sent by the DNS server.

This mechanism can help ensure that a single site for the host does not receive all the requests for the host. However, this mechanism does not provide the host address that is “best” for the client. The best address for the client is the one that has the highest proximity to the client, in terms of being the closest topologically, or responding the most quickly, and so on. Moreover, if a site is down, the simple round robin mechanism used by the DNS server cannot tell that the site is down and still sends that site’s host address on the top of the list. Thus, the client receives an address for a site that is not available and cannot access the requested host.

The ServerIron ADX GSLB feature solves this problem by intelligently using health checks and other methods to assess the availability and responsiveness of the host sites in the DNS reply, and if necessary exchanging the address at the top of the list with another address selected from the list. GSLB ensures that a client always receives a DNS reply for a host site that is available and is the best choice among the available hosts.

Basic concepts

The GSLB protocol is disabled by default. You must enable the GSLB protocol on each site ServerIron ADX. After you enable the GSLB protocol, the GSLB ServerIron ADX finds the site ServerIron ADXs using their IP management addresses, which you specify when you configure the remote site information. The GSLB controller ServerIron ADX front-ends the authoritative DNS server and provides the optimal IP address for the querying clients. Some or all of the IP addresses in the DNS response reside on site ServerIron ADX switches. The GSLB controller communicates with these ServerIron ADX switches designated as "site ServerIron ADX switches" in order to exchange and obtain information needed to evaluate IP addresses contained in the DNS responses.

The GSLB protocol is disabled by default on site ServerIron ADX switches. After you enable the GSLB protocol on site ServerIron ADX switches and configure the IP addresses of the site ServerIron ADX switches on the GSLB ServerIron ADX, then the GSLB ServerIron ADX establishes communication with the site ServerIron ADX switches.

The GSLB ServerIron ADX uses the GSLB protocol to learn the following information from the site ServerIron ADXs:

- **The VIPs configured on the site ServerIron ADXs and the health of the VIPs** —The site ServerIron ADXs report VIP additions and deletions asynchronously. Each time a VIP is added to a site ServerIron ADX, the ServerIron ADX sends a message to the GSLB ServerIron ADX to inform the GSLB ServerIron ADX of the change.

- **Session table statistics and CPU load information** — The site ServerIron ADXs report this information to the GSLB ServerIron ADX at regular intervals. By default, each remote ServerIron ADX sends the status information to the GSLB ServerIron ADX every 30 seconds. You can change the update period for all the remote ServerIron ADXs by specifying a new period on the GSLB ServerIron ADX if needed.
- **RTT** — Round Trip Time (RTT) is the amount of time that passes between when the remote site receives a TCP connection (TCP SYN) from the client and when the remote site receives the client's acknowledgment of the connection request (TCP ACK). The GSLB ServerIron ADX learns the RTT information from the site ServerIron ADXs through the GSLB protocol and uses the information as a metric when comparing site IP addresses.

  RTT information reported by site ServerIron ADXs is stored within prefix entries. In particular, the prefix entry holds the Client IP and prefix length. RTT entries are associated with this prefix entry and hold the site ServerIron ADX information and the corresponding RTT reported by this site ServerIron ADX for this prefix.
- **Connection load** — (Optional) A GSLB site's connection load is the average number of new connections per second on the site, over a given number of intervals. When you enable this GSLB metric, all potential candidates are compared against a predefined load limit. All sites that have fewer average connections than the threshold are selected and passed to the next comparison metric. The connection load metric is disabled by default but is enabled (added to the GSLB policy) when you configure the metric.

NOTE
All the ServerIron ADXs in the GSLB configuration (the GSLB ServerIron ADX and the remote site ServerIron ADX) must be running the same software release.

The GSLB ServerIron ADX uses the information supplied by the GSLB protocol when comparing the sites and may re-order the IP addresses in the authoritative DNS server's reply based on the results of the comparison. If you have enabled the GSLB protocol on the site ServerIron ADXs, the GSLB ServerIron ADX begins communicating with the site ServerIron ADXs using the GSLB protocol as soon as you add the site definitions to the GSLB ServerIron ADX.

When you configure the GSLB ServerIron ADX, you also specify the zones for which you want the ServerIron ADX to provide global SLB. These are the zones for which the DNS server (the one the ServerIron ADX is a proxy for) is the authority. In this example, the DNS server is an authority for brocade.com. Only the zones and host names you specify receive global SLB. The DNS server can contain other host names that are not globally load balanced or otherwise managed by the GSLB ServerIron ADX.

You also must specify the host names and applications that you want to provide global SLB for. For example, assume that brocade.com contains the following host names and applications.

www.brocade.com (HTTP)

ftp.brocade.com (FTP)

The application specifies the type of health check the GSLB ServerIron ADX applies to IP addresses for the host. A host name can be associated with more than one application. In this case, the GSLB ServerIron ADX considers a host name's IP address to be healthy only if the address passes all the health checks. The ServerIron ADX has Layer 7 health checks for the following applications:

- **FTP**: the well-known name for port 21. (Ports 20 and 21 both are FTP ports but on the ServerIron ADX, the name corresponds to port 21.)
- **TFTP**: the well-known name for port 69
- **HTTP**: the well-known name for port 80

- **IMAP4:** the well-known name for port 143
- **LDAP**: the well-known name for port 389
- **NNTP**: the well-known name for port 119
- **POP3:** the well-known name for port 110
- **SMTP**: the well-known name for port 25
- **TELNET**: the well-known name for port 23

NOTE
To display the list when configuring zone information, enter the **host-info** <*host-name*> ? command, where <*host-name*> is a string specifying a host name.

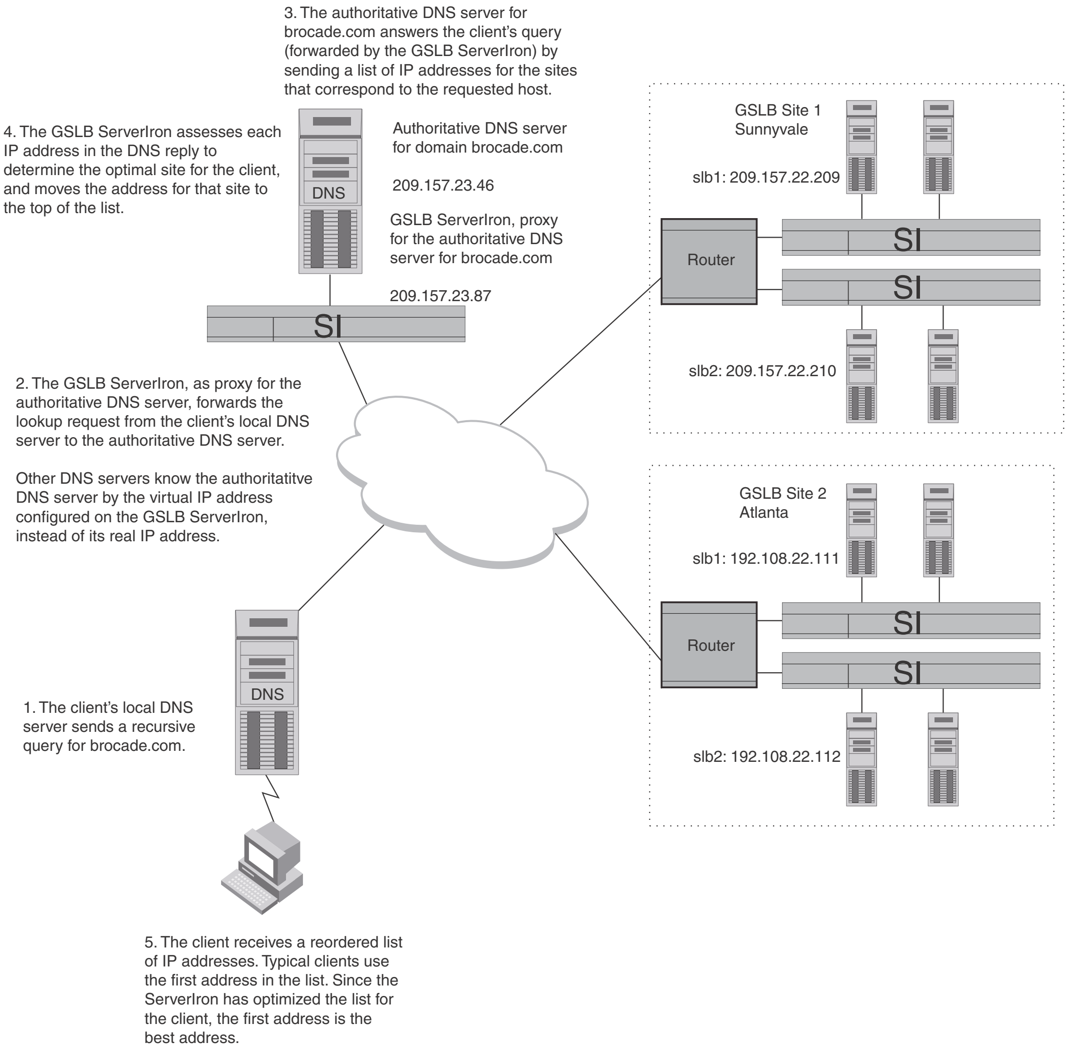
For other applications (applications not listed above), the ServerIron ADX does not perform a Layer 7 heath check but still performs a Layer 3 or Layer 4 TCP or UDP health check.

You can customize the HTTP health check on an individual host basis by changing the URL string the ServerIron ADX requests in the health check and the list of HTTP status codes the ServerIron ADX accepts as valid responses to the health check.

GSLB example

Figure 1 shows an example of a GSLB configuration. In this example, the GSLB ServerIron ADX (a ServerIron ADX configured for global SLB) is connected to the authoritative DNS server for a specific domain. (You can configure the ServerIron ADX for more than one domain; this example uses only one for simplicity.) The authoritative DNS server for brocade.com is known to other devices as 209.157.23.87. This is a VIP configured on the GSLB ServerIron ADX for the DNS server.

FIGURE 1 **Global Server Load Balancing configuration**



3. The authoritative DNS server for brocade.com answers the client's query (forwarded by the GSLB ServerIron) by sending a list of IP addresses for the sites that correspond to the requested host.

4. The GSLB ServerIron assesses each IP address in the DNS reply to determine the optimal site for the client, and moves the address for that site to the top of the list.

2. The GSLB ServerIron, as proxy for the authoritative DNS server, forwards the lookup request from the client's local DNS server to the authoritative DNS server.

Other DNS servers know the authoritatitve DNS server by the virtual IP address configured on the GSLB ServerIron, instead of its real IP address.

1. The client's local DNS server sends a recursive query for brocade.com.

5. The client receives a reordered list of IP addresses. Typical clients use the first address in the list. Since the ServerIron has optimized the list for the client, the first address is the best address.

This example shows a ServerIron ADX configured as a DNS proxy. The ServerIron ADX is configured as a DNS proxy for the DNS server that is authoritative for the domain brocade.com. To configure the ServerIron ADX as a DNS proxy, you identify the DNS name and configure a virtual IP address (VIP) for the DNS. Requests from clients or other DNS servers go to the VIP on the ServerIron ADX, not directly to the DNS server. The ServerIron ADX then sends the requests to the DNS server, transparently to the clients or other DNS servers.

NOTE

As an alternative to configuring the GSLB ServerIron ADX as a proxy, you can configure it to intercept and either redirect or directly respond to DNS queries. Refer to "DNS cache proxy" on page 91 and "Transparent DNS query intercept" on page 95.

The client's local DNS server might cache DNS replies from the authoritative server. Normally, these cached responses would prevent the global SLB from taking place, since the local DNS server would respond directly to the client without sending a recursive query to the authoritative DNS server. However, the GSLB ServerIron ADX, as a proxy for the authoritative DNS server, automatically resets the Time-to-Live (TTL) parameter in each DNS record from the authoritative server. By default, the GSLB ServerIron ADX sets the TTL to 10 seconds. As a result, other DNS servers that receive the records retain them in their databases for only 10 seconds. After the ten seconds expire, subsequent requests from the client initiate another query to the authoritative DNS server. As a result, the client always receives fresh information and the address of the site that is truly the best site for the client.

NOTE
You also can change the TTL if needed. However, Brocade recommends that you do not change the TTL to 0, because this can be interpreted as an error by some older DNS servers.

You identify each ServerIron ADX by its management IP address, not by any VIPs configured on the ServerIron ADX. Optionally, you also can specify a name for each ServerIron ADX at the site.

If a remote site is managed by one or more ServerIron ADXs, the GSLB ServerIron ADX gathers additional information from the site ServerIron ADXs using GSLB protocol with the remote ServerIron ADXs. The protocol uses TCP port 182. To initiate the GSLB protocol between the GSLB ServerIron ADX and the ServerIron ADXs at the remote sites, you must first enable the GSLB protocol on those remote ServerIron ADXs, then identify the sites and the ServerIron ADXs. In this example, the GSLB ServerIron ADX is configured with site information for Site 1 in Sunnyvale and Site 2 in Atlanta. Each site has servers containing the content for domain names within the domain brocade.com. The servers are load balanced by the ServerIron ADXs.

GSLB policy

The ServerIron ADX can use the following metrics to evaluate the server IP addresses in a DNS reply:

- The server’s health
- The weighted IP value assigned to an IP address
- The weighted site value assigned to a site
- The site ServerIron ADX’s remote SI session capacity threshold
- The IP address with the highest number of active bindings
- The round-trip time between the remote ServerIron ADX and the DNS client’s subnet
- The geographic location of the server
- The connection load
- The site ServerIron ADX’s available session capacity
- The site ServerIron ADX’s FlashBack speed (how quickly the GSLB receives the health check results)
- The site ServerIron ADX’s administrative preference (a numeric preference value you assign to influence the GSLB policy if other policy metrics are equal)
- The Least Response selection (the site ServerIron ADX that has been selected less often than others)
- Round robin selection (an alternative to the Least Response metric)

NOTE
The default order for the metrics is the order shown above.

The GSLB ServerIron ADX evaluates each IP address in the DNS reply based on these metrics. Based on the results, the GSLB ServerIron ADX can reorder the list to place the IP address for the “best” site on the top of the list.

If the GSLB policy rejects all of the sites, the GSLB ServerIron ADX sends the DNS reply unchanged to the client.

All of these metrics have default values but you can change the values if needed. In addition, you can disable individual metrics or reorder them. Refer to "Changing the GSLB policy metrics" on page 34.

You also can configure the GSLB ServerIron ADX to directly respond to DNS queries instead of forwarding the queries to the authoritative DNS server and modifying the replies. Refer to "DNS cache proxy" on page 91.

The following sections describe each of these metrics in detail.

Server health

The GSLB ServerIron ADX sends a Layer 3, Layer 4 TCP or UDP health check and Layer 7 application health check to the server to determine the health of the server and the host application on the server. If the server fails either health check, the GSLB ServerIron ADX immediately disqualifies the server's IP address from being the "best" site.

When you configure a ServerIron ADX for GSLB, it learns a series of IP addresses from its configured DNS real servers. Then it performs Layer 3, Layer 4, and if possible, Layer 7 health checks against those IP addresses.

The GSLB ServerIron ADX determines which health checks to use based on the host applications you specify. For example, if a host name is associated with both HTTP and FTP applications, the ServerIron ADX sends the site Layer 4 TCP health checks (one for HTTP and one for FTP) and also sends a separate Layer 7 HTTP health check and a separate Layer 7 FTP health check. The site must pass all the health checks or it is disqualified from being the best site.

If a host application uses a port number that is not known to the ServerIron ADX and supported by GSLB, the ServerIron ADX cannot perform a Layer 7 health check on the application but still performs a Layer 4 TCP or UDP health check on the port. Health check parameters such as retry interval, number of retries, and so on are global parameters.

NOTE
You can change the order in which the GSLB policy applies the metrics. However, Brocade recommends that you always use the health check as the first metric. Otherwise, it is possible that the GSLB policy will not select a "best" choice, and thus send the DNS reply unchanged. For example, if the first metric is geographic location, and the DNS reply contains two sites, one in North America and the other in South America, the GSLB policy favors the South American site after the first comparison. However, if that site is down, the GSLB policy will find that none of the sites in the reply is the "best" one, and thus send the reply unchanged.

NOTE
If all the sites fail their health checks, resulting in all the sites being rejected by the GSLB ServerIron ADX, the ServerIron ADX sends the DNS reply unchanged to the client.

Weighted IP metric

Beginning with software release 08.1.00R, you can configure the ServerIron ADX to distribute GSLB traffic among IP addresses in a DNS reply, based on weights assigned to the IP addresses. The weights determine the percentage of traffic each IP address receives in comparison with other candidate IP addresses, which may or may not have assigned weights.

NOTE
You cannot use the weighted IP metric if the weighted site metric is enabled.

The GSLB ServerIron ADX uses relative percentages in order to achieve 100% total weight distribution.

To configure weighted IP metrics, refer to “Implementing the weighted IP metric” on page 40.

Weighted site metric

You can configure the ServerIron ADX to distribute SLB traffic among GSLB sites based on weights configured for the sites. The weights determine the percentage of traffic each site will receive in comparison with other sites, which may or may not have weights.

NOTE
You cannot use the weighted site metric if the weighted IP metric is enabled.

You assign weights to GSLB sites. Each GSLB site may consist of one or more ServerIron ADXs, but the weight is applicable to the site as a whole.

The GSLB ServerIron ADX uses relative percentages in order to achieve 100% total weight distribution.

Site ServerIron ADX’s session capacity threshold

The GSLB protocol supplies statistics for the session tables on each site ServerIron ADX. The session table contains an entry for each open TCP or UDP session on the site ServerIron ADX. Each ServerIron ADX has a maximum number of sessions that it can hold in its session table. Through the GSLB protocol, the GSLB ServerIron ADX learns from each remote ServerIron ADX the maximum number of sessions and the number of available sessions on that ServerIron ADX.

The capacity threshold specifies how close to the maximum session capacity the site ServerIron ADX (remote ServerIron ADX) can be and still be eligible as the best site for the client. This mechanism provides a way to shift load away from a site before the site becomes congested.

The default value for the threshold is 90%. Thus a site ServerIron ADX is eligible to be the best site only if its session utilization is below 90%. refer to “Displaying GSLB information” on page 165 for commands to display a site’s utilization and the capacity threshold.

Active bindings metric

You can configure the ServerIron ADX to prefer an IP address with the highest number of active bindings.

Active bindings are a measure of the number of active real servers bound to a Virtual IP address (VIP) residing on a GSLB site. The GSLB ServerIron ADX uses the active bindings metric to select the best IP address for the client.   The VIP with the highest number of active bindings is the IP address preferred by the active bindings metric.

To configure active bindings metrics, refer to “Enabling the active bindings metric” on page 118.

Round-trip time between the remote ServerIron ADX and the client

The Round-trip time (RTT) is the amount of time that passes between when the remote site receives a TCP connection (TCP SYN) from the client and when the remote site receives the client's acknowledgment of the connection request (TCP ACK). The GSLB ServerIron ADX learns the RTT information from the site ServerIron ADXs through the GSLB protocol and uses the information as a metric when comparing site IP addresses.

The GSLB ServerIron ADX maintains a database of cache entries, which contains the information about past DNS queries. The information is aggregated on a network-address prefix basis. When the GSLB ServerIron ADX receives a DNS query, it creates or updates a cache entry. RTT measurements reported by remote ServerIron ADXs are then sorted into the cache. The GSLB ServerIron ADX uses this information for decisions on subsequent DNS queries. If a cache entry is not refreshed for a while (there are no subsequent queries from the same address prefix), the ServerIron ADX clears the entry from the RTT database.

When the GSLB ServerIron ADX compares two site IP addresses based on RTT, the GSLB ServerIron ADX favors one site over the other only if the difference between the RTT values is greater than the specified percentage. This percentage is the RTT tolerance. You can set the RTT tolerance to a value from 0-100. The default is 10%.

Site ServerIron ADXs send RTT information only for the sessions that clients open with them. To prevent the GSLB ServerIron ADX from biasing its selection toward the first site ServerIron ADX that sent RTT information, the GSLB ServerIron ADX intentionally ignores the RTT metric for a specified percentage of the requests from a given client network. You can specify an RTT explore percentage from 0-100. The default is 5. By default, the GSLB ServerIron ADX ignores the RTT for 5% of the client requests from a given network.

To configure RTT parameters, refer to "Modifying round-trip time values" on page 53.

Geographic location of the server

For each client query, the GSLB ServerIron ADX can determine the geographic location from which the client query came based on its IP address. The GSLB can determine whether the query came from North America, Asia, Europe, South America, or Africa.

If multiple sites compare equally based on the metrics above, the GSLB ServerIron ADX prefers sites within the same geographic region as the client query.

NOTE
The GSLB ServerIron ADX deduces the geographic region of the client's local DNS server from the destination IP address in the DNS reply, which is the address of the client's local DNS server.

The GSLB ServerIron ADX determines the geographic region of a server IP address in its DNS database in the following ways:

- For real IP addresses (as opposed to VIPs, which are logical IP addresses configured on the site ServerIron ADXs), the geographic region is based on the IP address itself.
- For VIPs, the geographic region is based on the management IP address of the site ServerIron ADX on which the VIP is configured.
- You can explicitly specify the region if the management IP address of the remote ServerIron ADX is not indicative of the geographic location. For example, if the management IP address is in a private subnet, the address does not indicate the ServerIron ADX's geographic location. If you specify the region, the ServerIron ADX uses the region you specify instead of the region of the ServerIron ADX's management IP address.

Site ServerIron ADX's connection load

A GSLB site's connection load is the average number of new connections per second on the site, over a given number of intervals. When you enable this GSLB metric, all potential candidates are compared against a predefined load limit. All sites that have fewer average connections than the threshold are selected and passed to the next comparison metric. The connection limit metric is disabled by default but is enabled (added to the GSLB policy) when you configure the metric.

Site ServerIron ADX's available session capacity tolerance

If multiple sites are equal after the above comparisons, the GSLB ServerIron ADX prefers the site ServerIron ADX (remote ServerIron ADX) whose session table has the most unused entries.

When comparing sites based on the session table utilization, the GSLB ServerIron ADX considers the sites to be equal if the difference in session table utilization does not exceed the tolerance percentage. The tolerance percentage ensures that minor differences in utilization do not cause frequent, and unnecessary, changes in site preference.

For example, suppose one ServerIron ADX has 1 million sessions available, and another has 800,000 sessions available. Also assume that the tolerance is 10% (the default). In this case the first ServerIron ADX (with 1 million sessions available) is preferred over the second ServerIron ADX because the difference (200,000) is greater than 10% of 1 million. If a third ServerIron ADX has 950,000 sessions available, that ServerIron ADX is equally preferable with the first ServerIron ADX (with 1 million sessions available), because the difference in percentage between the available sessions on the two ServerIron ADXs is only 5%, which is less than the tolerance threshold.

Site ServerIron ADX's FlashBack speed

If multiple sites compare equally based on all the metrics above, the ServerIron ADX chooses a site as the best one based on how quickly the GSLB ServerIron ADX received responses to health checks to the site ServerIron ADX.

The GSLB ServerIron ADX uses a tolerance value when comparing the FlashBack speeds of different sites. The tolerance value specifies the percentage by which the FlashBack speeds of the two sites must differ in order for the ServerIron ADX to choose one over the other. The default FlashBack tolerance is 10%. Thus, if the FlashBack speeds of two sites are within 10% of one another, the ServerIron ADX considers the sites to be equal. However, if the speeds differ by more than 10%, the ServerIron ADX prefers the site with the lower FlashBack speed.

FlashBack speeds are measured at Layer 4 for all TCP/UDP ports. For the application ports known to the ServerIron ADX, the FlashBack speed of the application is also measured.

When the ServerIron ADX compares the FlashBack speeds, it compares the Layer 7 (application-level) FlashBack speeds first, if applicable. If the application has a Layer 7 health check and if the FlashBack speeds are not equal, the ServerIron ADX is through comparing the FlashBack speeds. If a host is associated with multiple applications, the GSLB ServerIron ADX uses the slowest response time among the applications for the comparison. However, if only the Layer 4 health check applies to the application, or if further tie-breaking is needed, the ServerIron ADX then compares the Layer 4 FlashBack speeds.

Site ServerIron ADX's administrative preference

The administrative preference is an optional metric. This metric is a numeric preference value from 0-255 that you assign to each site ServerIron ADX, to select that ServerIron ADX if the previous metrics do not result in selection of a best site. The GSLB policy prefers the site ServerIron ADX with the highest administrative preference.

The administrative preference allows you to do the following:

- You can temporarily change the preference of a site to accommodate changing network conditions. For example, if sites are offering proxy content service, the link between a site proxy server farm and the content origin may be highly congested, making that site less desirable. This factor is not visible to the ServerIron ADXs and thus cannot be reflected in the other GSLB metrics.
- You can temporarily disqualify a site ServerIron ADX from being selected, without otherwise changing the site's configuration or the GSLB ServerIron ADX's configuration. For example, you can perform maintenance on the site ServerIron ADX without making network changes. In this case, set the administrative preference to 0.
- You can bias a GSLB ServerIron ADX that is also configured as a site ServerIron ADX (for locally configured VIPs) to always favor itself as the best site. In this case, assign an administrative preference of 255 to the site for the GSLB ServerIron ADX itself, and assign a lower administrative distance to the other site ServerIron ADXs, or use the default (128) for those sites.

The administrative preference is disabled by default, which means it is not included as one of the GSLB metrics. When you enable this metric, the default administrative preference for sites is 128. You can change the preference on an individual site basis. To change a site's preference, refer to "Configuring a site" on page 19.

The least response selection

If multiple sites still compare equally based on all the metrics above, the GSLB ServerIron ADX selects the site that it has selected least often before. For example, if the GSLB ServerIron ADX has selected Site 1 and placed its IP address on top in 40% of the DNS replies, but has selected Site 2 60% of the time, then in this instance the GSLB ServerIron ADX selects Site 1. To display the response selection percentages for the sites you have configured, use the **show gslb dns zone** command. Refer to "Displaying DNS zone and hosts" on page 170.

This metric is a tie-breaker in case multiple addresses pass through all the above comparisons without one address emerging as the best choice. If this occurs, the address of the site that has been selected least often in previous DNS responses is selected.

Least response selection is enabled by default. You can disable the metric only by enabling the round robin selection metric to act as the tie breaker instead. See the following section.

Round robin selection

The round robin selection metric is an alternative to the least response selection metric as the final tie breaker. When you enable round robin selection, the GSLB ServerIron ADX automatically disables the least response selection metric, and instead uses the round robin algorithm to select a site. round robin selection chooses the first IP address in the DNS response for the first client request, then selects the next address for the next client request, and so on.

Use the round robin selection metric instead of the least response selection metric when you want to prevent the GSLB ServerIron ADX from favoring new or recently recovered sites over previously configured active sites. The Least Response metric can cause the GSLB ServerIron ADX to select a new site or a previously unavailable site that has come up again instead of previously configured sites for a given VIP. This occurs because the GSLB ServerIron ADX has selected the new site fewer times than previously configured sites for the VIP.

In some cases, the least response selection metric can cause the GSLB ServerIron ADX to send client requests to a new or recovered site faster than the site can handle while it is coming up. To avoid this situation, you can configure the GSLB ServerIron ADX to use the round robin selection metric instead of the least response selection metric as the final tie breaker.

The round robin selection metric is disabled by default.

Check the current and maximum values for GSLB resources using the **show gslb resource** CLI command.

```
ServerIronADX# show gslb resources
    GSLB resource usage:
                        Current   Maximum
    sites               0         128
    SIs                 0         200
    SIs' VIPs           0         2048
    dns zones           0         1000
    dns hosts           0         1000
    health-checks app.  0         1000
    dns IP addrs.       0         2048
    affinities          0         1024
    affinity groups     0         128
    static prefixes     0         250
    user geo prefixes   0         512
    prefix cache        0         11786
    RTT entries         0         10000
    GSLB host policies  0         100
```

If you are configuring more than 256 zones or configuring more than 600 hosts, perform the following tasks.

1. Change the maximum virtual server system parameter to the maximum value supported in the current release. Use the **l4-virtual-server** command.

   For the current maximum virtual server value supported, see the table named "The Number of Supported Real Servers, Virtual Servers and Ports" in the *ServerIron ADX Server Load Balancing Guide*.

2. Change the maximum real server system parameter to the maximum value supported in the current release. Use the **l4-real-server** command.

   For the current maximum real server value supported, see the table named "The Number of Supported Real Servers, Virtual Servers and Ports" in the *ServerIron ADX Server Load Balancing Guide*.

3. Change the maximum server port parameter to the maximum value supported in the current release. Use the **l4-server-port** command.

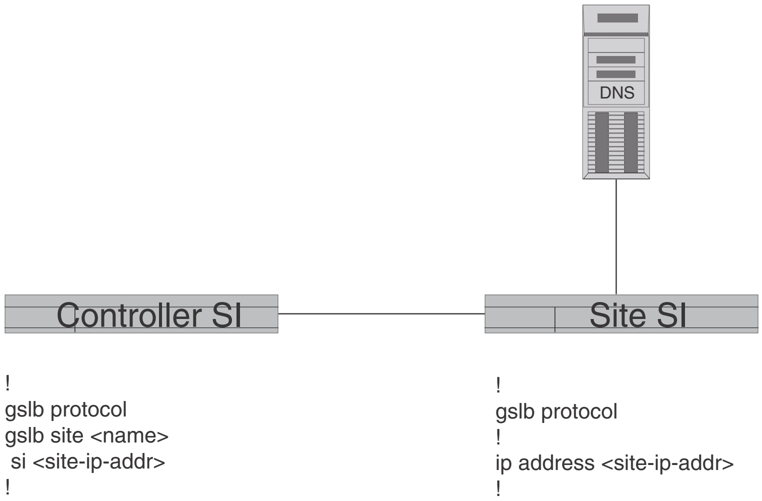
   For the current maximum server port value supported, see the table named "The Number of Supported Real Servers, Virtual Servers and Ports" in the *ServerIron ADX Server Load Balancing Guide*.

4. Check your system parameter values using the **show default value** CLI command.

NOTE
The sum of number of VIPs configured and the number of GSLB hosts configured on the GSLB ServerIron ADX should not exceed 1024. Similarly, the sum of real servers configured and the number of DNS IP addresses should not exceed 4096.

Minimum required configuration

FIGURE 2 Basic controller and site communication



```
!
gslb protocol
gslb site <name>
 si <site-ip-addr>
!
```

```
!
gslb protocol
!
ip address <site-ip-addr>
!
```

To add a DNS policy, you must also define the DNS real server and VIP on the ServerIron ADX as shown in the following example.

```
!
server real <dns-rs-name> <dns-ip-addr>
 port dns
 port dns zone "<domain-name>"
 port dns proxy
 port http
 port http url "HEAD /"
!
!
server virtual <dns-vs-name> <vip-ip-addr>
 port dns
 port http
 bind dns dns-rs dns
 bind http dns-rs http
!
gslb dns zone <domain-name>
 host-info www http
```

Use **server real** *<dns-rs-name> <dns-ip-addr>* for a local DNS server. Use **server remote-name** *<dns-rs-name> <dns-ip-addr>* for a remote DNS server. The **host-info** defines an enabled application in the DNS zone. For example, you can also specify **host-info ftp ftp**.

Issue **show gslb site** on the controller to display site communication information. The state displays “CONNECTION ESTABLISHED” when communication is successful. A protocol version of 1 corresponds to “ATTEMPTING CONNECTION”. Established connections use protocol versions 4 or 5.

```
SLB-chassis(config)# show gslb site

SITE: brocade
  Enhanced RTT smoothing: OFF

SI: 1.1.1.1:
state: ATTEPTING CONNECTION
Protocol Version: 1
Active RTT gathering: NO
Secure Authenticate/Encrypt: NO
```

To display the default settings, enter the following command (Note the default metric processing order).

```
Default metric order: ENABLE
Metric processing order:
              1-Server health check
              2-Remote SI's session capacity threshold
              3-Round trip time between remote SI and client
              4-Geographic location
              5-Remote SI's available session capacity
              6-Least response selection


DNS active-only: DISABLE  DNS best-only: DISABLE  DNS override: DISABLE
DNS cache-proxy: DISABLE  DNS transparent-intercept: DISABLE
DNS cname-detect: DISABLE  Modify DNS response TTL: ENABLE
DNS TTL: 10 (sec), DNS check interval: 30 (sec)
Remote SI status update period: 30 (sec)
Remote SI health-status update period: 5 (sec)
Session capacity threshold: 90%  Session availability tolerance: 10%
Round trip time tolerance: 10%, round trip time explore percentage: 5%
Round trip time cache prefix: 20, round trip time cache interval: 120 (sec)
Round trip time cache age refresh: DISABLE
Round trip time algorithm selection:  USE PASSIVE ONLY
Connection load: DISABLE
Weighted Site Metric: DISABLE     Weighted IP Metric: DISABLE
Active Bindings Metric: DISABLE
```

Syntax: **show gslb policy**

Configuring GSLB

The examples in the procedures in this section are based on the configuration shown in Figure 1 on page 4.

TABLE 1 Configuration tasks: Global SLB

Feature	See page...
DNS proxy parameters	
Configure a source IP address. The source IP address is required so that the GSLB ServerIron ADX can perform the health checks on remote devices. Add a real-server definition for the DNS server. Add a VIP for the DNS server and bind the real server and virtual server.	page 17
Site parameters	
Enable the GSLB protocol on each remote ServerIron ADX.	page 19
Specify the sites and the ServerIron ADXs within the sites.	page 19
Zone parameters	
Specify the zones and the host names within the zones.	page 21
Private Virtual IPs (VIPs) (optional)	
Enable a site ServerIron ADX to communicate public VIP addresses to a GSLB ServerIron ADX.	
GSLB parameters (optional)	
Change the GSLB protocol port number (optional).	page 29
Change the GSLB protocol update period (optional).	page 30
Modify the GSLB parameters related to DNS responses.	page 30
GSLB Policy Metrics	
Change the order of GSLB policy metrics	page 37
Disable or enable GSLB policy metrics	page 38
Clear the DNS selection counters for GSLB metrics	
Configure the weighted IP metric	
Configure the weighted site metric	
Configure the active bindings metric	
Modify connection load parameters	page 49
Modify Session Table capacity and Threshold Tolerance values	page 51
Modify Flashback tolerance values	page 52
Modify round-trip time (RTT) values	page 53
Affinity (optional)	
Configure the ServerIron ADX to always favor a specific site based on client IP address	page 85
DNS cache proxy (optional)	
Configure the ServerIron ADX to directly respond to DNS queries	page 91
Transparent DNS query intercept (optional)	
Configure the ServerIron ADX to intercept and redirect DNS queries	page 95

TABLE 1 Configuration tasks: Global SLB (Continued)

Feature	See page...
Disable or re-enable GSLB Traps (optional)	
Disable or re-enable GSLB SNMP traps and syslog messages	page 186
GSLB Error Handling for Unsupported DNS Requests (optional)	
Configure the ServerIron ADX to send error messages in response to client requests for unsupported DNS record types.	page 188

You can configure the GSLB ServerIron ADX to be a proxy for more than one DNS server.

As shown in the example in Figure 1 on page 4, you implement GSLB by connecting a ServerIron ADX to an authoritative DNS server. To configure the ServerIron ADX for GSLB, perform the following steps:

- Add the proxy information for the DNS server. To configure the GSLB ServerIron ADX as a proxy for the DNS server, add real server definition for the DNS server, then add a virtual server (VIP) for the DNS server and bind the real and virtual servers.

  NOTE
  The virtual server IP address (VIP) will be the Authoritative DNS server for the GSLB Domain.

- If a site contains ServerIron ADXs, identify the server sites. A server site is a data center or server farm connected to the Internet by a router. This example shows two GSLB sites. Each of the sites is connected to the Internet by a router.
- If a site contains ServerIron ADXs, identify the ServerIron ADXs within the server sites. This initiates the GSLB protocol between the ServerIron ADX acting as a DNS proxy and the remote ServerIron ADXs in the GSLB sites. The DNS proxy uses information supplied by the remote ServerIron ADXs to assess the preferability of IP addresses in the DNS replies.

  NOTE
  You can use the GSLB ServerIron ADX for standard SLB. In this case, identify the local site and the GSLB ServerIron ADX in the same way as you identify the other sites and ServerIron ADXs. The configuration steps are the same.

- Identify the DNS zones and the hosts within those zones for which you want the GSLB ServerIron ADX to perform GSLB. You must specify the zones and hosts. There are no defaults.
- Identify the host applications with each host. The GSLB ServerIron ADX performs GSLB for the applications you specify. You can specify applications known to the ServerIron ADX as well as the TCP or UDP port numbers of applications that are not known to the ServerIron ADX. The ServerIron ADX performs Layer 7 and Layer 4 health checks for the applications known to the ServerIron ADX, but performs only Layer 4 health checks for applications that are not know to it. Refer to "Server health" on page 7.

Proxy for DNS server

NOTE
The following scenario is for switch software. If you are using router software, then all you need is an interface IP on the ServerIron ADX that can reach the DNS server.

To configure the GSLB ServerIron ADX as a proxy for a DNS server, complete the following steps.

1. If the GSLB ServerIron ADX and site ServerIron ADXs are in different subnets, add a source IP address. In this case, the source IP address is required so that the GSLB ServerIron ADX perform the health checks on the IP addresses the GSLB ServerIron ADX learns from the DNS server for which it is the proxy. The source IP address must be in the same subnet as the GSLB ServerIron ADX's management IP address.

   NOTE
   You can specify as many DNS servers as the GSLB ServerIron ADX's system memory allows. However, the ServerIron ADX sends periodic DNS queries to only the first four DNS servers you configure with the DNS proxy.

   If you configure the ServerIron ADX as a proxy for multiple DNS servers, make sure they have identical content for the zones that you configure the GSLB ServerIron ADX to provide GSLB services for.

2. Add a real server for the DNS server.
3. Add a virtual server for the DNS server and bind the real DNS server and virtual server together.

Adding a source IP address

To enable the GSLB ServerIron ADX to perform health checks on remote sites that are in a subnet other than the GSLB ServerIron ADX's subnet, you must add a source IP address to the GSLB ServerIron ADX. The source IP address must be in the same subnet as the GSLB ServerIron ADX's management IP address.

NOTE
If the DNS server for which the GSLB ServerIron ADX is a proxy is in a different subnet than the GSLB ServerIron ADX's management IP address, you can use the same source IP address that you add for the site ServerIron ADXs. However, you also need to enable the Source NAT feature for the DNS real server.

The source IP address and source NAT feature allow the ServerIron ADX to send a Layer 4 or Layer 7 health check to the remote site and receive the response. Notice that the source IP address added to the ServerIron ADX is not in the subnet of the remote ServerIron ADX. Instead, the source IP address is in the subnet that connects the ServerIron ADX's local router to the Internet. The purpose of the source IP address in this configuration is to ensure that the responses from remote sites come back to the ServerIron ADX. The health check packets use the address you configure as their source IP address. Without the source IP address in the ServerIron ADX's subnet and the source feature, the responses to the health checks sent to remote sites in different subnets cannot reach the ServerIron ADX.

For example, the GSLB ServerIron ADX shown in Figure 1 on page 4 needs a source IP address in the subnet 209.157.23.x. Without this source IP address, Layer 4 and Layer 7 health checks to the ServerIron ADXs at the Sunnyvale site (209.157.22.x) and the Atlanta site (192.108.22.x) cannot reach the GSLB ServerIron ADX.

To add a source IP address, enter a command such as the following:

```
ServerIronADX(config)# server source-ip 209.157.23.225 255.255.255.0 0.0.0.0
```

Syntax: [no] server source-ip <*ip-addr*> <*ip-mask*> <*default-gateway*>

The <*ip-addr*> parameter specifies the IP address. Specify an address that is in the same subnet as the GSLB ServerIron ADX's management IP address. Do not specify an address that is already in use.

The <*ip-mask*> parameter specifies the network mask.

The <*default-gateway*> parameter specifies the default gateway. This parameter is required, but if you do not want to specify a gateway, enter "0.0.0.0".

Configuring real server and virtual server for the DNS server

NOTE
The virtual server IP address (VIP) will be the Authoritative DNS server for the GSLB Domain.

To configure a real server and virtual server and bind them together for a proxy DNS server, enter commands such as the following:

```
ServerIronADX(config)# server real-name dns_ns 209.157.23.46
ServerIronADX(config-rs-dns_ns)# port dns proxy
ServerIronADX(config-rs-dns_ns)# exit
ServerIronADX(config)# server virtual-name-or-ip dns-proxy 209.157.23.87
ServerIronADX(config-vs-dns-proxy)# port dns
ServerIronADX(config-vs-dns-proxy)# bind dns dns_ns dns
```

The commands in this example add a real server called "dns_ns". The DNS server has IP address 209.157.23.46. When you add the real server, the CLI changes to the Real Server configuration level. At this level, you can add TCP or UDP ports and, optionally, modify health check parameters. In this example, the DNS port is added. Notice that the **proxy** option is specified following the **dns** option. The **proxy** option is required to indicate that this real server is part of a proxy DNS server configuration.

If the DNS server is in a different subnet than the GSLB ServerIron ADX, you must configure a source IP address on the ServerIron ADX for use by the health checks. If the GSLB ServerIron ADX is in a one-armed configuration or the DNS server is at least one hop away, you must configure a source IP address and also enable source NAT. (You do not need to add another source IP address if you have already added one for the remote sites. The GSLB ServerIron ADX can use the same source IP address for reaching the remote sites and for reaching the DNS server.)

```
ServerIronADX(config)# server real-name dns_ns 209.157.23.46
ServerIronADX(config-rs-dns_ns)# port dns proxy
ServerIronADX(config-rs-dns_ns)# exit
```

The **server virtual-name-or-ip** command adds a virtual server called "dns-proxy". This command changes the CLI to the Virtual Server configuration level. At this level, the **port dns** command adds the DNS port to the virtual server. The **bind** command binds the DNS port on the real server to the DNS port on the virtual server.

Syntax: [no] server real-name <*text*> <*ip-addr*>

Syntax: [no] port dns proxy

Syntax: [no] port <*port*> [disable | enable]

Syntax: [no] port <*port*> [keepalive]

Syntax: [no] server virtual-name-or-ip <*text*> [<*ip-addr*>]

Syntax: [no] bind <*port*> <*real-server-name*> <*port*>

Enabling the GSLB protocol

For security, remote ServerIron ADXs do not listen to TCP port 182 (the GSLB protocol port) by default. This means the GSLB protocol is disabled on remote site ServerIron ADXs by default. For a remote ServerIron ADX to use the protocol, you must enable the protocol on the remote ServerIron ADX (not the GSLB controller).

To enable the GSLB protocol on the site ServerIron ADXs, enter the following command.

```
ServerIronADX(config)#gslb protocol
```

Syntax: [no] gslb protocol

The ServerIron ADX uses TCP port 182 for the GSLB protocol by default. You can change the port number if needed. Refer to "Changing the protocol port number" on page 29.

You also can secure access to a ServerIron ADX by configuring Access Control Lists (ACLs). For example, you can configure ACLs to control access to the device on TCP port 182. See the "Access Control Lists (ACLs)" chapter of the *ServerIron ADX Security Guide.*

Configuring a site

When you create a site, you give it a name and identify the ServerIron ADXs in it. You can also enable the administrative preference.

To configure the server sites shown in Figure 1 on page 4, enter commands such as the following:

```
ServerIronADX(config)# gslb site sunnyvale
ServerIronADX(config-gslb-site-sunnyvale)# si-name slb-1 209.157.22.209
ServerIronADX(config-gslb-site-sunnyvale)# si-name slb-2 209.157.22.210
ServerIronADX(config)# gslb site atlanta
ServerIronADX(config-gslb-site-atlanta)# si-name slb-1 192.108.22.111
ServerIronADX(config-gslb-site-atlanta)# si-name slb-2 192.108.22.112
```

These commands configure two GSLB sites: one in Sunnyvale, the other in Atlanta. Each site contains two ServerIron ADXs, slb-1 and slb-2, that load balance traffic across server farms. The GSLB ServerIron ADX you are configuring will use information provided by the other ServerIron ADXs when it evaluates the servers listed in DNS replies.

To set the administrative preference for a site ServerIron ADX to 255, enter a command such as the following:

```
ServerIronADX(config-gslb-site-sunnyvale)# si-name slb-1 209.157.22.20 255
```

To change the preference for a site ServerIron ADX you have already configured, use the same command syntax. You do not need to reconfigure other site parameters when you change the preference. For example, to change the preference for a site ServerIron ADX from the default (128) to 200, enter a command such as the following:

```
ServerIronADX(config-gslb-site-sunnyvale)# si-name slb-2 209.157.22.210 200
```

NOTE
The administrative preference metric is disabled by default, which means it is not used by the GSLB policy. The GSLB policy uses the preference values only if you enable this metric. Refer to "Disabling or re-enabling individual GSLB policy metrics" on page 38.

Syntax: [no] **gslb site** <*name*>

The <*name*> parameter is a text string that uniquely identifies the site on the GSLB ServerIron ADX. You can enter a string up to 16 characters long. The string can contain blanks. To use blanks, enclose the string in quotation marks.

Syntax: [no] **si-name** [<*name*>] <*ip-addr*> [<*preference*>]

The **si-name** <*name*> parameter specifies a unique name for the ServerIron ADX at the site. You can enter a string up to 16 characters long. The string can contain blanks. To use blanks, enclose the string in quotation marks. You can enter up to four pairs of ServerIron ADX names and IP addresses on the same command line. The name is optional.

The <*ip-addr*> parameter specifies whether the remote site runs on the switch code or router code. If the remote site runs the switch code, enter the IP address configured on the site ADX. If it runs the router code, then enter the VE IP address on the site ADX.

In both cases, you must not enter a virtual IP address (VIP) configured on the ServerIron ADX or a source IP address added for source NAT.

The <*preference*> parameter sets the administrative preference for the site. When you enable the administrative preference as a GSLB metric, the administrative preference can be used by the GSLB policy when comparing this site with other sites. You can specify a preference from 0-255. The default preference is 128. The GSLB policy prefers high preference values over low preference values. If you specify 0, the site is administratively removed from selection by the GSLB policy but remains connected to the network. Refer to "Site ServerIron ADX's administrative preference" on page 11 for information about uses for this parameter.

NOTE
If the GSLB ServerIron ADX itself is also a site for a host, the configuration steps are the same as for remote site ServerIron ADXs. Add a site definition and then specify the GSLB ServerIron ADX as the ServerIron ADX at the site. Specify the management IP address as the ServerIron ADX IP address.

NOTE
If traffic between the GSLB ServerIron ADX and a remote site ServerIron ADX must pass through a firewall, the firewall must be configured to allow traffic to and from the GSLB ServerIron ADX.

Specifying site locations

By default, the GSLB ServerIron ADX uses a site's IP address to determine its geographic location. Alternatively, you can explicitly specify the location, by entering commands such as the following:

```
ServerIronADX(config)# gslb site sunnyvale
ServerIronADX(config-gslb-site-sunnyvale)# geo-location n-america
```

Syntax: [no] **geo-location asia** | **europe** | **n-america** | **s-america** | **africa**

Specifying GSLB controller locations

By default, the GSLB controller is assigned to the North America geographic. Specify the GSLB controller location by entering the following command at the global configuration level.

```
ServerIronADX(config)# gslb default-location asia
ServerIronADX(config)# write memory
```

Syntax: [no] **gslb default-location asia** | **europe** | **n-america** | **s-america** | **africa**

If GSLB default location is not specified and if the requesting client prefix is from an unknown geography, then the GSLB controller assigns "north-america" as its geography. However, if the default location is specified, the GSLB controller assigns the configured geography to unknown client prefixes.

NOTE
This command needs a reload, therefore, issue the **write memory** command after configuring the command.

Configuring a zone

You must specify the DNS zone name and the host information (applications) within each zone for which you want the GSLB ServerIron ADX to provide global SLB. There are no defaults for these parameters. As soon as you specify the hosts and applications, the GSLB ServerIron ADX queries the DNS server (the one for which the GSLB ServerIron ADX is a proxy) for the IP addresses associated with the hosts and begins sending health checks to the hosts.

To configure a zone, enter commands such as the following:

```
ServerIronADX(config)# gslb dns zone-name brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# host-info ftp ftp
```

This example adds the zone brocade.com and two host names within that zone: www and ftp. The GSLB ServerIron ADX will provide global SLB for these two hosts within the zone.

Syntax: [no] **gslb dns zone-name** <*name*>

The <*name*> parameter specifies the DNS zone name. If you delete a DNS zone (by entering no gslb dns zone-name <*name*>), the zone and all the host names you associated with the zone are deleted.

Syntax: [no] **host-info** <*host-name*> <*host-application*> | <*TCP/UDP-port-num*>

The <*host-name*> parameter specifies the host name. You do not need to enter the entire (fully-qualified) host name. Enter only the host portion of the name. For example, if the fully qualified host name is *www.brocade.com*, do not enter the entire name. Enter only “www”. The rest of the name is already specified by the gslb dns zone-name command. You can enter a name up to 32 characters long.

The <*host-application*> parameter specifies the host application for which you want the GSLB ServerIron ADX to provide global SLB. You can specify one of the following:

- **FTP**: the well-known name for port 21. (Ports 20 and 21 both are FTP ports but on the ServerIron ADX, the name “FTP” corresponds to port 21.)
- **TFTP**: the well-known name for port 69
- **HTTP**: the well-known name for port 80

- **IMAP4**: the well-known name for port 143
- **LDAP:** the well-known name for port 389
- **NNTP:** the well-known name for port 119
- **POP3:** the well-known name for port 110
- **SMTP**: the well-known name for port 25
- **TELNET**: the well-known name for port 23

The <*TCP/UDP-port-num*> parameter specifies a TCP/UDP port number instead of a well-known port. If the application is not one of those listed above, you still can configure the GSLB ServerIron ADX to perform the Layer 4 health check on the specified port. If the application number does not correspond to one of the well-known ports recognized by the ServerIron ADX, the GSLB ServerIron ADX performs Layer 4 TCP or UDP health checks for the ports but does not perform application-specific health checks.

Applying GSLB to CNAME records

A Canonical Name (CNAME) record is a type of DNS record that allows network administrators to create aliases for domain names. For example, an administrator can create the following DNS records for the Brocade domain:

- **Address record**: *www.brocade.com*, IP address 209.157.22.241
- **CNAME record**: *www.brocade.com,* alias for *www.brocade.com*

A CNAME record refers to another domain name instead of an IP address. A client can enter either domain name to get to the site. In this example, each domain name goes to site 209.157.22.241.

GSLB supports CNAME records. If you configure domain names that map to other domain names, the GSLB ServerIron ADX still will perform GSLB for the domain.

By default, the ServerIron ADX applies the GSLB policy only to zone and application names that are configured on the ServerIron ADX. Thus, if the ServerIron ADX receives a DNS reply that contains CNAME records for the requested zone and application, the ServerIron ADX does not apply the GSLB policy to the CNAME records.

You can enable the ServerIron ADX to search its GSLB database for the zone and application names in CNAME records. For example, if the ServerIron ADX receives a DNS reply that contains the CNAME record *www.brocade.com*, and the zone and application name "*www.brocade.com*" have been configured on the ServerIron ADX, the ServerIron ADX will apply the GSLB policy to the CNAME record.

To enable the ServerIron ADX to apply GSLB to CNAME records, enter the following commands.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns cname-detect
```

Syntax: [no] dns cname-detect

NOTE
This feature does not apply to cache proxy GSLB or transparent intercept GSLB.

To display the status of CNAME, enter the following command.

```
ServerIronADX(config-gslb-policy)# show gslb policy

  Default metric order: ENABLE
  Metric processing order:
                1-Remote ServerIronADX's session capacity threshold
                2-Round trip time between remote ServerIronADX and client
                3-Geographic location
                4-Remote ServerIronADX's available session capacity
                5-Least response selection


  DNS active-only: DISABLE  DNS best-only: DISABLE  DNS override: DISABLE
  DNS cache-proxy: DISABLE  DNS transparent-intercept: DISABLE
  DNS cname-detect: ENABLE   Modify DNS response TTL: ENABLE
  DNS TTL: 10 (sec), DNS check interval: 30 (sec)
  Remote ServerIronADX status update period: 30 (sec)
  Session capacity threshold: 90%, session capacity tolerance: 10%
  Round trip time tolerance: 10%, round trip time explore percentage: 5%
  Round trip time cache prefix: 20, round trip time cache interval: 120 (sec)
  Connection load: DISABLE
```

The CNAME status is shown in bold type.

Syntax: **show gslb policy**

Configuring HTTP health check parameters

For HTTP hosts, you also can customize the health check by changing the URL method and the string requested by the ServerIron ADX, as well as the HTTP status codes the ServerIron ADX accepts as valid responses. By default, the ServerIron ADX performs the HTTP health check as follows:

- The ServerIron ADX sends a HEAD request for the default URL string, “HEAD /”.
- If the server responds with the status code 401 or a code in the range 200-299, the server passes the health check.

You can change the request method from HEAD to GET. In addition, you can change the URL string the ServerIron ADX requests from the server and the status codes that the ServerIron ADX accepts as valid responses for passing the health check.

The commands in the following example change the method from HEAD to GET and to add 404 as a valid status code response to the health check.

```
ServerIronADX(config)# gslb dns zone brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http url "GET
/index.htm"
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http status-code 200
299 401 401 404 404
```

Syntax: **host-info** <*host-name*> **http** | <*TCP-portnum*> **url “[GET** | **HEAD]** [/]<*URL-page-name*>

GET or **HEAD** is an optional parameter that specifies the request type. By default, HTTP keepalive uses HEAD to retrieve the URL page. You can override the default and configure the ServerIron ADX to use GET to retrieve the URL page.

The slash (/) is an optional parameter. If you do not set the GET or HEAD parameter, and the slash is not in the configured URL page, then ServerIron ADX automatically inserts a slash before retrieving the URL page.

Syntax: **host-info** <*host-name*> **http** | <*TCP-portnum*> **status-code** <*range*> *[<range>* [<*range*> [<*range*>]]]

You can specify up to four ranges (total of eight values). To specify a single message code for a range, enter the code twice. For example to specify 200 only, enter the following command: **port http status-code 200 200**.

NOTE
When you change the status code ranges, the defaults are removed. As a result, you must specify all the valid ranges, even if a range also is within the default ranges. For example, if you still want codes 200-299 to be valid, you must specify them.

NOTE
When a URL string is associated with a TCP port number rather than the well-known HTTP port, the ServerIron ADX performs both a TCP and an HTTP health check. In this case, you must specify the method and URL before specifying the status code ranges. The software displays an error message if you accidentally try to change the status codes before specifying the method and URL.

Configuring DNS domain name aliases

You can configure an alias for a domain name and application configured on the GSLB ServerIron ADX. This feature is useful together with the DNS cache proxy feature when you want the GSLB ServerIron ADX to learn a set of proxy server IP addresses for a domain, then respond to client requests with the best proxy server address.

Typically, you use this set of features when the DNS server contains a single server address for the actual domain name, but a separate set of proxy server addresses for an alias for that domain name. When you enable DNS cache proxy and configure the alias for the domain on the GSLB ServerIron ADX, the GSLB ServerIron ADX:

- Learns the proxy server addresses under the alias on the DNS server instead of the address for the domain's actual site. This requires configuration of the alias on the GSLB ServerIron ADX.
- Responds to client queries for the actual domain name with the best site address from among the proxy server addresses learned from the DNS server under the alias. This requires that enable the DNS cache proxy feature.

NOTE
Use this feature only in conjunction with the DNS cache proxy feature. Otherwise, it is possible for the IP address(es) the ServerIron ADX learns under the real domain name and the addresses it learns under the alias to be different. When this is the case, the ServerIron ADX does not make any alterations to the DNS response but instead sends the response back to the client unaltered. As a result, the ServerIron ADX sends the client the DNS reply with the real domain name's server address, instead of one of the proxy addresses configured on the DNS server under the domain's alias.

To configure an alias for a domain name, enter the alias after entering the zone name and host application names, as in the following:

```
ServerIronADX(config)# gslb dns zone brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host www http
ServerIronADX(config-gslb-dns-brocade.com)# host www alias www.gslb.brocade.com
```

The commands configure a zone called "*brocade.com*", associate an HTTP host named "*www*" with the zone, then associate the alias "*www.gslb.brocade.com*" with the host and zone.

Syntax: **host-info** <*host-name*> **alias** <*alias-name*>

NOTE
Make sure you configure the alias only after configuring the zone and the host application the alias is for, as shown in the example above. In addition, make sure you specify the fully-qualified name for the alias (for example, "*www.gslb.brocade.com*" instead of "*www.gslb*".

Configuring null host names

When you configure a zone name in GSLB, you enter the zone name, then associate host applications with the zone name. For example, you might configure the following for the "brocade.com" zone:

- **www.brocade.com** (HTTP application)
- **ftp.brocade.com** (FTP application)

Some e-commerce sites also accept just a zone name as an alias for a specific application within that zone. For example, a site might accept both "*www.brocade.com*" and "brocade.com" as valid names for the HTTP application on the web host. In this case, the second name has a null host name. No application is explicitly associated with the "brocade.com" zone, but the DNS server is configured to associate "brocade.com" with the same IP address(es) and application as "*www.brocade.com*", for example using address records or alias records.

NOTE
The real Authoritative DNS server must be configured to support Null Host.

To configure a null host name, enter commands such as the following:

```
ServerIronADX(config)# gslb dns brocade-name brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# host-info null-host http
```

The last command in the example above configures a null host for the brocade.com zone and associates the null host with HTTP.

Syntax: **[no] host-info** <*host-name*> **| null-host** <*host-application*> **|** <*TCP/UDP-port-num*>

You can configure one null host for each application and zone name.

Configuration example

Here is a proxy server configuration example for a GSLB ServerIron ADX.

To configure the ServerIron ADX as a DNS server proxy, enter commands such as the following:

```
ServerIronADX(config)# server real-name dns_ns 192.10.10.1
ServerIronADX(config-rs-dns_ns)# port dns proxy
ServerIronADX(config-rs-dns_ns)# exit
ServerIronADX(config)# server virtual-name-or-ip dns-proxy 192.10.10.69
ServerIronADX(config-vs-dns-proxy)# port dns
ServerIronADX(config-vs-dns-proxy)# bind dns dns_ns dns
```

The commands configure the GSLB ServerIron ADX as the proxy for the client's DNS server.

The following commands configure the zone and host information for brocade.com and specify the IP address of the proxy server.

```
ServerIronADX(config)# gslb dns zone brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# host-info www ip-list 209.157.23.59
```

When the ServerIron ADX receives a reply from the client's DNS server for brocade.com, the ServerIron ADX replaces the IP address in the reply with 209.157.23.59, the IP address of a proxy server.

DNS override allows the ServerIron ADX to replace the IP address in the DNS reply with the IP address you configure for the proxy server.

The following commands enable DNS override on the ServerIron ADX.

```
ServerIronADX(config-vs-dns-proxy)# exit
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns override
```

Syntax: **dns override**

You must enable DNS override for the ServerIron ADX to replace the address. Otherwise, the ServerIron ADX still uses the GSLB policy to select a "best" site but does not replace the IP address with the proxy server's address. The **gslb policy** command changes the CLI to the GSLB policy configuration level.

Private VIPs for GSLB

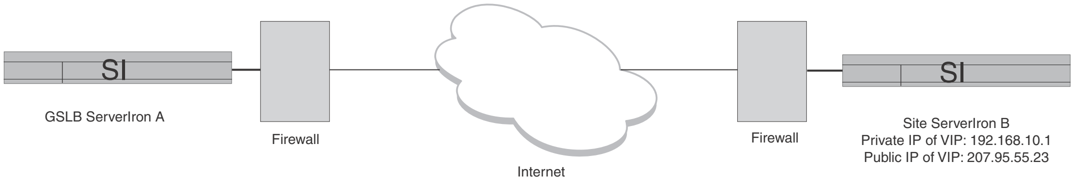
ServerIron ADX supports private Virtual IP (VIP) configurations for GSLB. GSLB support for private VIPs enables a site ServerIron ADX to communicate public VIP addresses to a GSLB ServerIron ADX, and, in effect, the GSLB ServerIron ADX to recognize these IP addresses in the DNS reply, as VIPs on the site ServerIron ADX. This is accomplished by statically mapping the private and public IP address for a VIP on the site ServerIron ADX.

Note that each time the mapping between the private IP address of the VIP and the public IP address changes, you need to reconfigure the new public IP address for the VIP on the ServerIron ADX, as well. Also, the GSLB IP addresses apply only to the GSLB feature. GSLB IP addresses do not affect any other feature nor are they used by any other feature.

For example, as illustrated in Figure 3, suppose 192.168.10.1 is the private IP address of the VIP on ServerIron ADX B, and it is mapped to 207.95.55.23 by the firewall. On ServerIron ADX B, you would statically map the GSLB public IP address of 207.95.55.23 for the private VIP 192.168.10.1. You would also specify whether this public IP address is for use only by the peer GSLB ServerIron ADX A, or if it will be used by both the peer GSLB ServerIron ADX A and ServerIron ADX B, if a local GSLB site is present.

After statically mapping the public IP address, ServerIron ADX B will then communicate the public VIP address, 207.95.55.23 to the peer GSLB ServerIron ADX A. If GSLB ServerIron ADX A is providing global SLB for the domain *www.foo.com*, where one of the IP addresses corresponding to this domain is 207.95.55.23, then GSLB ServerIron ADX A will correctly interpret this IP address as a VIP on the site ServerIron ADX B.

FIGURE 3 GSLB and private VIPs



Using the example in Figure 3, suppose the configuration specifies that the public IP address will be used by both the peer GSLB ServerIron ADX A and the site ServerIron ADX B. If ServerIron ADX B is providing GSLB in addition to being a site ServerIron ADX, and has a local site configured, then it will also use this public IP address of the VIP for its local site.

Configuring a public IP address for a VIP

To configure a public IP address for a VIP that will be used only by the peer GSLB ServerIron ADX, but not for a local site (if present), by the ServerIron ADX itself, enter commands such as the following:

```
ServerIronADX-B# config t
ServerIronADX-B(config)# server virtual-name-or-ip dns-test 192.168.10.1
ServerIronADX-B(config-vs-dns-test)# gslb-ip 207.95.55.23 for-peer-only
ServerIronADX-B(config-vs-dns-test)# exit
```

To configure a public IP address for a VIP that will be used both by the peer GSLB ServerIron ADX and locally, by the ServerIron ADX itself (if a local GSLB site is present), enter commands such as the following:

```
ServerIronADX-B# config t
ServerIronADX-B(config)# server virtual-name-or-ip dns-test 192.168.10.1
ServerIronADX-B(config-vs-dns-test)# gslb-ip 207.95.55.23 for-self-and-peer
ServerIronADX-B(config-vs-dns-test)# exit
```

Note that these are the commands you would enter for the example shown in Figure 3.

Syntax: **gslb-ip** *<IP address>* *<for-peer-only* | *for-self-and-peer>*

The *<IP address>* is the public IP address for the VIP.

The *<for-peer-only>* parameter specifies that only the peer GSLB ServerIron ADX will use this public VIP address. The ServerIron ADX will continue to use the private IP address of the VIP for the local site, if present.

The *<for-self-and-peer>* parameter specifies that both the peer GSLB ServerIron ADX and the local ServerIron ADX will use this public IP address for the VIP.

NOTE
Each time the mapping between the private IP address of the VIP and the public IP address changes, you need to reconfigure the new public IP address for the VIP on the ServerIron ADX, as well. Also, the GSLB IP addresses apply only to the GSLB feature. GSLB IP addresses do not affect any other feature nor are they used by any other feature.

Private VIP display information

To obtain more information about the public and private IP addresses configured for a VIP on a ServerIron ADX, use the following commands:

- **show gslb dns zone** (see "Displaying the results of traffic distribution for Weighted IPs" on page 42 for an example screen display)
- **show gslb site** (see "Displaying GSLB IP information" on page 28)
- **show gslb dns detail** (the following is an example)

```
ServerIronADX# show gslb dns detail

ZONE: gslb1.com
HOST: www:
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*    10.10.10.200: dns v-ip    ACTIVE N-AM      9   19    0 (0%)
                  site: sunnyvale, weight:   0, ServerIronADX: 10.10.10.100
                  session util:   0%, avail. sessions: 524274
                  preference: 128
                  Metric counter (count [selection-metric]):
                  Not selected yet

*       1.1.1.101: dns v-ip    ACTIVE N-AM      0    0    4 (100%)
                  IP weight: 50
                  Active Bindings: 1
                  site: sanjose, weight:   0, ServerIronADX: 1.1.1.254
                  session util:   0%, avail. sessions: 5999979
                  preference: 128
                  Metric counter (count [selection-metric]):
                  4[weighted-ip]
```

For information about the field definitions for these commands, see the ServerIron ADX.

Displaying GSLB IP information

You can view the GSLB IP address configuration for a VIP on a ServerIron ADX. You can display information about the public IP address for the ServerIron ADX, to see whether the public IP address is used by both the local and peer GSLB ServerIron ADXs, or by the peer GSLB ServerIron ADX only.

To display public IP address information, enter the following command.

```
ServerIronADX-B# show server virtual-name-or-ip
Virtual Servers Info

Name: dns-test               State: Enabled             IP:192.168.10.1:   1
Pred: least-conn             ACL-Id: 0                  TotalConn: 0
GSLB IP: 207.95.55.23 (use for local and remote)

Port    State     Sticky  Concur  Proxy  DSR   CurConn  TotConn  PeakConn
----    -----     ------  ------  -----  ---   -------  -------  --------

default enabled   NO      NO      NO     NO    0        0        0
http    enabled   NO      NO      NO     NO    0        0        0
```

The display shows that the public IP address, 207.95.55.23, is used by both the local and peer GSLB ServerIron ADXs.

Syntax: show server virtual-name-or-ip

NOTE
For a complete description of the fields shown in this screen display, refer to the ServerIron ADX.

To display the IP address used for a VIP at a given GSLB site, enter the following command.

```
ServerIronADX-B# sh gslb site

SITE: local

ServerIronADX:   192.168.10.7:
state: SELF
Protocol Version: 2
distributed health-chk

 Current num.  Session   CPU load  Preference  Location  Connection
 sessions      util(%)   (%)       (0-255)               Load-Avg
           12        0          4         128  N-AM           --

 Virtual IPs: 207.95.55.23(A)
```

The example shows that the public IP address, 207.95.55.23, is used for the VIP at the site "local" on the ServerIron ADX.

Syntax: show gslb site

NOTE
For a complete description of the fields shown in this screen display, refer to the ServerIron ADX.

Configuring GSLB protocol parameters

This section describes how to modify the following GSLB protocol parameters:

- GSLB protocol port number: refer to "Changing the protocol port number" on page 29.
- GSLB protocol update period: refer to "Changing the GSLB protocol update period" on page 30.
- DNS response parameters: refer to "Modifying GSLB parameters related to DNS responses" on page 30.
- GSLB policy parameters: refer to "Changing the GSLB policy metrics" on page 34.

Changing the protocol port number

By default, a GSLB ServerIron ADX uses TCP port 182 to exchange GSLB information with other ServerIron ADXs, including the site ServerIron ADXs.

For example, if other devices in the network also use port 182, but for other applications, you need to change the protocol on those devices or on the ServerIron ADXs.

To change the GSLB protocol port, enter the following command.

```
ServerIronADX(config)#gslb communication 1882
```

Syntax: [no] gslb communication <*tcp-portnum*>

The <*tcp-portnum*> parameter specifies the TCP port number you want the ServerIron ADX to use for exchanging GSLB information with other ServerIron ADXs.

If you change the GSLB protocol port number, you must write memory and reload the software to place the change into effect. Also, you must change the port to the same number on all ServerIron ADXs in the GSLB configuration. If the port number in two GSLB ServerIron ADXs is not the same, those ServerIron ADXs are not able to properly perform GSLB.

Changing the GSLB protocol update period

The GSLB protocol update period specifies how often the site ServerIron ADXs report their session table statistics and CPU utilization to the GSLB ServerIron ADX. The default update period is 30 seconds.

By default, each remote ServerIron ADX uses the GSLB protocol to send status information to the GSLB ServerIron ADX every 30 seconds. The status information consists of session utilization and CPU load information, which you can display using the **show gslb site** command (refer to "Displaying site information" on page 165).

You can change the period to a value from 1-300 seconds. The GSLB ServerIron ADX then informs all the remote ServerIron ADXs of the change.

To change the GSLB protocol update period, enter the following commands on the GSLB ServerIron ADX.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# protocol status-interval 10
```

The command changes the GSLB protocol update period to 10 seconds.

Syntax: **[no] protocol status-interval** <*num*>

The <*num*> parameter specifies the number of seconds between status reports and can be from 1-300 seconds. The default is 30 seconds.

To display the current update period, enter the **show gslb policy** command. The interval is shown in the Remote ServerIron ADX status update period field. Refer to "Displaying the default GSLB policy" on page 175 for more information.

Modifying GSLB parameters related to DNS responses

You can modify the following DNS-related GSLB parameters:

- **IP address for a site that fails a health check:** refer to "Removing IP addresses for sites that fail a health check" on page 31.
- **IP addresses that pass the health checks but still are not selected as the "best" site:** By default, the ServerIron ADX leaves all the IP addresses in the DNS reply. You can configure the ServerIron ADX to remove all addresses from the reply except the "best" address. Refer to "Removing all addresses except the best address" on page 31.
- **DNS record verification interval:** refer to "Changing the query interval" on page 32.
- **TTL value the ServerIron ADX sets for the DNS records:** refer to "Changing the TTL for DNS records" on page 32.
- If you prefer to manage the TTL values solely using the DNS server, you can disable TTL modification on the ServerIron ADX. refer to "Disabling TTL modification" on page 32.
- **DNS override:** refer to "Enabling DNS override" on page 33.

Removing IP addresses for sites that fail a health check

By default, the ServerIron ADX does not remove an IP address from a DNS reply even if the address fails a health check.

You can configure the ServerIron ADX to remove IP addresses from DNS replies when those addresses fail a health check. The ServerIron ADX removes the addresses that fail the check so long as the DNS query still contains at least one address that passes the health check.

A site must pass all applicable health checks (Layer 4 and Layer 7) to avoid being removed.

NOTE
If all the sites fail their health checks, resulting in all the sites being rejected by the GSLB ServerIron ADX, the ServerIron ADX sends the DNS reply unchanged to the client.

When DNS active policy is enabled, there is a case where a client will still get an IP that failed a health check. Therefore, when an IP list for a zone is configured, you need to also configure DNS override on the GSLB policy.

The GSLB default behavior is as follows:

- In DNS proxy, the entire list of IP addresses is sent back to the client with the best IP address selected by the controller at the top of the list. This best IP is selected in accordance with the GSLB policy. An administrator typically configures active only, because the LDNS may cache this response for TTL time and may round robin the IPs in this list in some cases.
- Health check in the GSLB policy is disabled. Typically administrators will not disable health check if they are using active only.
- Active only applies only to the remaining IP addresses in the list, not the best one. An administrator should enable health check for best IP selection to ensure that best IP is healthy.

To configure the ServerIron ADX to remove IP addresses from DNS replies when those addresses fail a health check, enter the following commands.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns active-only
```

Syntax: [no] dns active-only

Removing all addresses except the best address

By default, the GSLB ServerIron ADX retains the same number of IP addresses in the DNS replies from the DNS server. The GSLB policy swaps the IP address on the top of the list with the “best” address, selected by the GSLB policy. You can configure the ServerIron ADX to remove all addresses except the one the GSLB policy selects as the best address.

NOTE
If the GSLB policy does not result in the selection of a “best” address, the DNS reply can still contain multiple addresses.

To configure the GSLB ServerIron ADX to remove all addresses except the best address from the DNS replies, enter the following commands.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns best-only
```

Syntax: [no] dns best-only

To display the state of this feature, enter the **show gslb policy** command. The DNS best-only field indicates whether the feature is enabled or disabled. Refer to "Displaying the default GSLB policy" on page 175.

Changing the query interval

Frequency with which the ServerIron ADX verifies its current DNS records with DNS servers. As soon as you add site and host information for GSLB, the ServerIron ADX sends DNS queries to the DNS server (the one for which the ServerIron ADX is the proxy) to get the IP addresses associated with the zones and host names you specified. After this, the ServerIron ADX refreshes this information by sending new DNS queries every 30 seconds. You can change the query interval.

The GSLB ServerIron ADX periodically sends DNS queries to verify the zone and host information. The GSLB ServerIron ADX sends the queries to the DNS server for which it is configured to be a proxy. The default interval is 30 seconds. You can change the interval to a value from 0-1000000000 seconds.

To change the refresh interval, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns check-interval 50
```

Syntax: [no] **dns check-interval** <*num*>

The <*num*> parameter specifies the interval and can be from 1-1000000000 seconds. The default is 30 seconds.

Changing the TTL for DNS records

By default, the ServerIron ADX sets the TTL to 10 seconds in the DNS records in all the replies from the DNS server for which the ServerIron ADX is performing GSLB. The TTL controls how long other DNS servers, including the client's DNS server, keep the query results in their databases. You can change this TTL.

NOTE
We recommend that you do not change the TTL to 0, because this can be interpreted as an error by some older DNS servers.

The GSLB ServerIron ADX changes the TTL of each DNS record contained in the DNS replies from the DNS server for which the ServerIron ADX is a proxy. By default, the GSLB ServerIron ADX changes the TTL to 10. You can modify this to a value from 0-1000000000 seconds.

To change the TTL, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns ttl 45
```

Syntax: [no] **dns ttl** <*num*>

The <*num*> parameter specifies the TTL and can be from 0-1000000000 seconds. The default is 10 seconds.

For all GSLB features except DNS cache proxy, the command **dns ttl** configures the ServerIron ADX to use the TTL from the DNS server. If you are using DNS cache proxy, this command resets the TTL to 10.

Disabling TTL modification

If you prefer to manage the TTL values solely on the DNS server and do not want the ServerIron ADX to modify the TTL, you can disable TTL modification. To do so, enter the following command.

```
ServerIronADX(config-gslb-policy)# no dns ttl
```

Syntax: [no] dns ttl

Enabling DNS override

By default, the GSLB ServerIron ADX selects the best site IP address from among the addresses contained in the DNS reply. You can override the DNS reply for an individual domain (zone plus a host) by specifying a list of IP addresses, then enabling DNS override. The GSLB controller replies with all available IP addresses for the respective domain with best IP address on top of the list.

DNS override is useful when you want to provide the best address for a web proxy without the need to configure the proxy's IP address onto the DNS server itself.

DNS override is a global parameter. You configure redirection on an individual host basis, then globally enable the GSLB ServerIron ADX to replace the IP addresses in the DNS reply with the proxy server addresses you configure.

Once you configure DNS override, for each domain name (zone and host) configured on the GSLB ServerIron ADX, there must be a set of IP addresses configured for the domain. The GSLB ServerIron ADX replaces the IP addresses in a DNS response with the best choice (only the best choice) from the set of configured IP addresses. If a domain name does not have a configured address, the ServerIron ADX sends the DNS reply unaltered to the client.

NOTE
The host and its associated health check (if applicable) must be configured before you configure the IP address list.

You can specify as many proxy server IP addresses as you need for a given domain. When you specify multiple proxy server addresses, the ServerIron ADX uses the applicable GSLB policy metrics to select the best address from the list of addresses you configure and places that address in the DNS reply.

To configure the proxy server information on the GSLB ServerIron ADX, enter commands such as the following:

```
ServerIronADX(config)# gslb dns zone brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# host-info www ip-list 209.157.23.59
```

Syntax: **host-info** <*host-name*> **ip-list** {<*ipv4-address*> | <*ipv6-address*>

The <*host-name*> parameter specifies the host name.

The **ip-list** <*ipv4-address*> *and* <*ipv6-address*> variables specify the proxy IPv4 or IPv6 address(es). You can specify as many proxy IP addresses as you need. If you specify multiple addresses, separate each address with a space. Here is an example.

```
host-info www ip-list 209.157.23.59 209.157.23.60 209.157.23.61 207.142.33.6
```

For information about the other syntax for the **host** command, refer to "Configuring a zone" on page 21.

To enable DNS override, enter the following command. You must enable DNS override to allow the ServerIron ADX to insert the proxy IP address in the DNS reply.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns override
```

Syntax: [no] dns override

When you enable DNS override, the GSLB ServerIron ADX replaces the IP addresses in the DNS reply with the “best” of the proxy server addresses you specify. The GSLB ServerIron ADX determines which proxy server IP address is the best using the GSLB policy metrics. For information about the metrics, refer to “GSLB policy” on page 6.

NOTE
DNS override is a global parameter but a list of proxy IP addresses are associated with a specific host in a specific domain. If there are no proxy addresses for a given host, the GSLB ServerIron ADX sends the DNS reply unaltered. An exception is if you have enabled the active only feature, in which case the reply contains only the active addresses. Refer to “Removing IP addresses for sites that fail a health check” on page 31.

To display the DNS override state, enter the **show gslb policy** command. The state is shown in the DNS override field. Refer to “Displaying the default GSLB policy” on page 175 for more information.

To display information about the IP addresses selected for a specific domain and host, enter the **show gslb dns zone** command. Refer to “Displaying DNS zone and hosts” on page 170.

Changing the GSLB policy metrics

“GSLB policy” on page 6 describes the default policy the GSLB ServerIron ADX uses to evaluate the IP addresses in the DNS replies from the DNS server for which the ServerIron ADX is configured as a proxy. You can change the policy by changing or deleting individual metrics. Table 2 lists the GSLB policy metrics. The metrics are listed in their default order. The metric described in the first row is the first metric the GSLB ServerIron ADX uses by default, and so on.

For example, you can change the following:

- **Metric processing order:** you can change the order in which the metrics are applied.
- **Metric state:** you can disable or re-enable some metrics.
- **Session-table capacity and threshold tolerance:** you can modify the values for these metrics.
- **FlashBack tolerance**: you can modify the value for this metric.
- **RTT values:** you can individually modify the cache interval, cache prefix, tolerance, and explore percentage.
- **Connection load parameters**: you can adjust the number of data collection intervals and the relative weights given to the intervals.

NOTE
If the GSLB policy rejects all of the sites, the GSLB ServerIron ADX sends the DNS reply unchanged to the client.

TABLE 2 GSLB policy metrics

Metric	Default	Configuration options
Server (host) health	**Enabled.** The GSLB ServerIron ADX performs Layer 4 health checks on the TCP or UDP port and Layer 7 health checks on the application, if the application is known to the ServerIron ADX. NOTE: If all the sites fail their health checks, resulting in all the sites being rejected by the GSLB ServerIron ADX, the ServerIron ADX sends the DNS reply unchanged to the client.	You can disable this metric. NOTE: When both the health check metric and the Flashback metric are disabled, the ServerIron ADX does not perform any Layer 4 or Layer 7 health checks.
Weighted IP metric	**Disabled.** When enabled, the ServerIron ADX distributes GSLB traffic among IP addresses in a DNS reply, based on weights assigned to the IP addresses.	You can enable this metric and assign weights to individual IP addresses. The weight can be from 0 to 100. The default is 0. You can disable this metric.
Weighted site metric	**Disabled.** When the weighted IP metric is enabled, the weighted site metric is disabled. The weighted site metric is an alternative to the weighted IP metric. They are mutually exclusive. When enabled, the ServerIron ADX distributes SLB traffic among GSLB sites based on weights configured for the sites.	You can enable this metric and assign weights to individual sites. The weight can be from 0 to 100. The default is 0. You can disable this metric.
Session capacity threshold	**Enabled.** The default value for the threshold is 90%. Thus a site ServerIron ADX is eligible to be the best site only if its session utilization is below 90%.	You can change the threshold to a value from 0-100%. You can disable this metric.
Active bindings metric	**Disabled.** When enabled, the ServerIron ADX selects an IP address with the highest number of active bindings as the best IP address for the client.	You can enable and disable this metric.
Round-trip time (RTT) from remote ServerIron ADXs to the DNS clients.	**Enabled.** The default RTT cache interval is 120 seconds. The default cache prefix length is 20 bits. The default tolerance (used when comparing otherwise equal sites) is 10%. The default explore percentage is 5%.	You can change the RTT cache interval, cache prefix length, tolerance, and explore percentage individually. You can disable this metric. If you disable RTT, the GSLB ServerIron ADX instructs the site ServerIron ADXs to stop sending RTT information.
Geographic location	**Enabled.**	You can disable this metric.

TABLE 2 GSLB policy metrics (Continued)

Metric	Default	Configuration options
Connection load	**Disabled.**	You can enable this metric. You also can change the data collection interval, the number of intervals used to calculate the connection load average, and the relative weights of the intervals.
Available session capacity	**Enabled.** The default tolerance is 10%. When comparing sites based on the session table utilization, the GSLB ServerIron ADX will prefer one site over the other only if the difference in session table utilization is greater than the tolerance percentage.	You can change the tolerance to a value from 0-100%. You also can disable this metric.
FlashBack speed (how quickly the GSLB receives the Layer 4 TCP and Layer 7 health check results)	**Disabled.** The default tolerance is 10%. This applies to the TCP health check and application health checks. When comparing sites based on the FlashBack speed, the GSLB ServerIron ADX will prefer one site over the other only if the FlashBack speeds differ by more than the specified tolerance.	You can change the TCP and application tolerances individually. A change applies to all the TCP ports or applications at the remote site. You also can disable this metric.
Administrative preference	**Disabled.** When enabled, the default preference is 128. The GSLB ServerIron ADX will prefer the site with the highest administrative preference. If you set the preference for a site ServerIron ADX to 0, the site is administratively removed from GSLB selection.	You can enable this metric. On an individual site ServerIron ADX basis, you can change the preference from 128 (the default) to a value from 0-255.
Least Response selection (the site ServerIron ADX that has been selected less often than others)	**Enabled.**	Not configurable.
Round robin selection	**Disabled.** When round robin selection is enabled, least response selection is disabled. round robin selection is an alternative to least response selection. They are mutually exclusive. Like least response selection, round robin selection is a tie breaker, used only if two or more sites are equal following comparison against all other enabled metrics.	Not configurable.

After changing policy values, you can display the new values using the **show gslb policy** command. If you decide you want to change a value back to its default (using "**no**" in front of the command you used to change it), you can display all the default policy values by entering the **show gslb default** command. Refer to "Displaying the default GSLB policy" on page 175.

NOTE
You also can configure the ServerIron ADX to intercept or directly respond to DNS queries instead of evaluating responses from the authoritative DNS server. Refer to "DNS cache proxy" on page 91 and "Transparent DNS query intercept" on page 95.

Changing the order of GSLB policy metrics

You can change the order in which the GSLB ServerIron ADX applies the policy metrics.

NOTE
We recommend that you always use the health check as the first metric. Otherwise, it is possible that the GSLB policy will not select a "best" choice, and thus send the DNS reply unchanged. For example, if the first metric is geographic location, and the DNS reply contains two sites, one in North America and the other in South America, for clients in South America the GSLB policy favors the South American site after the first comparison. However, if that site is down, the GSLB policy will find that none of the sites in the reply is the "best" one, and thus send the reply unchanged.

You cannot change the position of the least response selection or round robin selection metric, whichever is enabled. The GSLB ServerIron ADX uses the least response selection or round robin selection metric as a tie-breaker if the other comparisons do not result in selection of a "best" site.

To change the order, specify the metrics in the desired order, by entering a command such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# metric-order set health-check round-trip-time
capacity num-session flashback
```

This command changes the GSLB policy to the following:

- The health-check results
- The round-trip time between the remote ServerIron ADX and the DNS client
- The site ServerIron ADX's session capacity threshold
- The site ServerIron ADX's remote SI session capacity threshold
- The site ServerIron ADX's FlashBack speed (how quickly the GSLB receives the health check results)
- The Least Response selection (the site ServerIron ADX that has been selected less often than others)

Two of the metrics, server health and geographic location, are not specified. As a result, these metrics are not used when evaluating site IP addresses in the DNS responses.

Syntax: [no] metric-order set <*list*>

The <*list*> parameter is a list of the metrics you want to use, in the order you want the GSLB ServerIron ADX to use them. The GSLB uses the metrics in the order you specify them. You can specify one or more of the following:

- **active bindings:** The ServerIron ADX's preference for the IP address with the highest number of active bindings.
- **capacity**: The remote ServerIron ADX's session capacity threshold.
- **connection-load:** The site ServerIron ADX's average number of new connections per second
- **flashback:** The site ServerIron ADX's FlashBack speed (how quickly the GSLB receives the health check results)
- **geographic:** The geographic location of the server
- **health-check**: The Layer 4 and application health checks
- **num-session**: The remote ServerIron ADX's available session capacity
- **preference**: The administratively configured preference for the site ServerIron ADX
- **round-trip-time**: The round-trip time between the remote ServerIron ADX and the DNS client
- **weighted ip**: The administratively configured traffic distribution method for the ServerIron ADX
- **weighted site:** The administratively configured traffic distribution method for the ServerIron ADX

There are no parameters for the least response selection or round robin selection metrics. These metrics are tie-breakers. Only one of them is enabled at a time and the one that is enabled is always the last metric in the policy.

To reset the order of the GSLB policy metrics to the default (and also re-enable all disabled metrics), enter the following command.

```
ServerIronADX(config-gslb-policy)# metric-order default
```

Syntax: **metric-order default**

The **no metric-order set** command also resets the order and re-enables all disabled metrics. This command is equivalent to the **metric-order default** command.

To display the GSLB policy after you change it, enter the **show gslb policy** command. Refer to "Displaying the user-configured GSLB policy" on page 177.

Disabling or re-enabling individual GSLB policy metrics

You can explicitly disable individual GSLB policy metrics. For example, to disable the health check and geographic metrics, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# no health-check
ServerIronADX(config-gslb-policy)# no geographic
```

Syntax: [no] **health-check** | **num-session** | **preference** | **round-robin** | **round-trip-time** | **geographic** | **connection-load limit** <*average-load*> | **capacity** | **flashback**

The <*average-load*> parameter can be from 1 to as high a value as you need. There is no default. You must specify a connection limit to enable the connection limit metric.

NOTE
If you explicitly disable both the health check and FlashBack metrics, the GSLB ServerIron ADX does not perform any health checks on the remote sites. If you disable the RTT metric, the GSLB ServerIron ADX instructs the site ServerIron ADXs to stop sending RTT information.

To enable a metric, enter the command without "no" in front of it. For example, to re-enable both the metrics disabled in the preceding example, enter the following commands.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# health-check
ServerIronADX(config-gslb-policy)# geographic
```

To enable the administrative preference metric, which is disabled by default, enter the following commands.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# preference
```

To specify the site connection limit and enable the connection limit metric, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# connection-load limit 500
```

This command sets the site connection limit to 500 connections. During site comparison, the GSLB policy discards sites that have an average load of new connections that is higher than the amount you specify. All other sites are passed to the next GSLB policy metric as potential candidates.

Clearing DNS selection counters

The GSLB ServerIron ADX maintains DNS selection statistics for each IP address based on DNS requests served for a particular domain name. These DNS selection statistics include:

- How many times the IP address was selected as the best IP address
- Which metrics were used for making the IP address selection
- The percentage of times an IP address was selected in comparison with other IP addresses in the same domain name

Use the **show gslb dns zone** command to display the DNS selection statistics.

DNS selection statistics are used to implement GSLB metrics such as least response, weighted site and weighted IP metrics. Each of these metrics base subsequent selections on the number of times the IP address was previously selected. For example, the weighted site metric selects the IP address that has the least relative weight, the calculation of which is based on the selection counter of that IP address.

It can be advantageous to use the Clear DNS Selection Counters feature in conjunction with GSLB metrics. Consider the following examples:

- The Least Response metric selects the IP address that has been selected the least number of times when compared to other IP addresses. If an IP address has become available after having been down for some time, it might suddenly become flooded with subsequent traffic because its selection counter is low. Clearing the counters for that zone can prevent a flood to this IP address.
- You can also use this feature to test the GSLB implementation before deploying it on a wider scale. You can analyze the effectiveness of each GSLB metric by rearranging the metric order and using the Clear Counters feature to start over without having to reload the software.

To clear DNS selection counters globally or per zone, without reloading the software, or to clear out any DNS requests for any client, enter a command such as the following:

```
ServerIronADX# clear gslb dns zone zone1
```

Syntax: **clear gslb dns zone-name** [<*name*>]

Replace <*zone-name*> with the zone for which you want to clear the DNS selection counters. To clear the counters globally (for all zones), do not enter a <*zone-name*>.

Implementing the weighted IP metric

Beginning with router software release 08.1.00R, you can configure the ServerIron ADX to distribute GSLB traffic among IP addresses in a DNS reply, based on weights assigned to the IP addresses. The weights determine the percentage of traffic each IP address receives in comparison with other candidate IP addresses, which may or may not have assigned weights.

NOTE
You cannot use the weighted IP metric if the weighted site metric is enabled.

The GSLB ServerIron ADX uses relative percentages in order to achieve 100% total weight distribution, as shown in Table 3 and Table 4. In Table 3, the total of the Configured weighted IP metrics (2nd column) is 100. The last column shows that the GSLB ServerIron ADX distributes the traffic to the IP addresses exactly as configured. In this example, traffic distribution is straightforward because the total weight of all three IP addresses equals 100.

TABLE 3 Example weighted IP metric configuration

IP address	Configured weighted IP metric	Relative weighted IP metric
1.1.1.80	50	50%
1.1.2.80	30	30%
1.1.3.80	20	20%
Total	100	100%

Now consider the example in Table 4. In this example, the total of the Configured weighted IP metrics (2nd column) does not equal 100. However, as illustrated in the last column, the GSLB ServerIron ADX uses relative percentages in order to achieve 100% total weight distribution.

TABLE 4 Example weighted IP metric configuration

IP address	Configured weighted IP metric	Relative weighted IP metric
1.1.1.80	15	33% (15/45 x 100)
1.1.2.80	20	44% (20/45*100)
1.1.3.80	10	22% (10/45*100)
Total	45	100%

The weighted IP metric is disabled by default. When enabled, it is placed second in the GSLB algorithm, after the Health Check metric. You can change the metric order and enable or disable other metrics, although we do not recommended this.

DNS response processing

When the weighted IP metric option is enabled, the GSLB ServerIron ADX assesses each IP address in the DNS reply and selects the best IP address for a client, based on the weighted IP metrics configured in the GSLB policy.

Using the weighted IP metric, the GSLB algorithm calculates a relative weight for each IP address and selects the IP address with the least relative weight. The following criteria is used to calculate the relative weight of an IP address:

- The number of times the GSLB ServerIron ADX selected the IP address as the best IP address to reply to a client

- The number of eligible IP addresses to be evaluated by the weighted IP metric and their weights
- The weight assigned to the IP address

If an IP address has a relative weight of zero, or if it does not have a weight assigned to it, the IP address is not selected as the best IP address for a client.

If two or more IP addresses have the same relative weight, or if all of the IP addresses have a relative weight of zero, all of the IP addresses with the same relative weight are passed on to the next step in the GSLB algorithm, where the process of selecting the best IP address continues.

Configuring weighted IP metrics

To configure weighted IP metrics, complete the following tasks.

1. Enable the weighted IP metric.
2. Assign weights to the IP addresses.

For example, to enable the weighted IP metric, add the zone gslb.com, add the host www within the gslb.com zone, and assign a weight of 50 to the IP address 1.1.1.80, enter commands such as the following:

```
SLB-ServerIronADX(config-gslb-policy)# weighted-ip
SLB-ServerIronADX(config-gslb-policy)# gslb dns zone gslb.com
SLB-ServerIronADX(config-gslb-dns-gslb.com)# host www http
SLB-ServerIronADX(config-gslb-dns-gslb.com)# host www ip-weight 1.1.1.80 50
```

Syntax: [no] weighted-ip

Syntax: [no] gslb dns zone <*name*>

For <*name*>, enter up to 32 characters

Syntax: [no] host-info <*host-name*> <*host-application*> **|** <*tcp/udp-portnum*>

The <*host-name*> parameter specifies the host name. You do not need to enter the entire fully qualified host name. Enter only the host portion of the name. For example, if the fully qualified host name is *www.gslb.com*, do no enter the entire name. Enter only "www". The rest of the name is already specified by the **gslb dns zone** command.

The <*host-application*> parameter specifies the host application for which you want to create an IP list. Specify one of the following:

- **ftp**: the well-known name for port 21. (Ports 20 and 21 both are FTP ports but on the ServerIron ADX, the name “ftp” corresponds to port 21.)
- **tftp**: the well-known name for port 69
- **http:** the well-known name for port 80
- **imap4:** the well-known name for port 143
- **ldap**: the well-known name for port 389
- **nntp**: the well-known name for port 119
- **pop3**: the well-known name for port 110
- **smtp:** the well-known name for port 25
- **telnet:** the well-known name for port 23

The <*tcp/udp-portnum*> parameter specifies a TCP/UDP port number instead of a well-known port.

Syntax: host-info www ip-weight <*IP address*> <*weight*>

<*IP address*> is the IP address for which you are assigning a weight.

<*weight*> is a value from 0 to 100. The default value is 0.

However, this command will result in an error if the IP argument for ip-weight has not been previously entered as an argument for ip-list. For example, enter the command such as the following:

```
SLOWANSI01(config-gslb-dns-myzone.com)#host-info www ip-weight 4.4.4.4 80
```

This command will respond with the error message: "IP-address not found for host-name".

NOTE
If there is no 'ip-list' defined for the host, then the 'ip-weight' for the host IPs are removed from the 'gslb dns zone' configuration whenever the GSLB ServerIron ADX or the backend DNS servers are reloaded.

Displaying the results of traffic distribution for Weighted IPs

To view the results of traffic distribution after configuring weighted IP metrics, enter the following command.

```
ServerIronADX# show gslb dns zone

ZONE: gslb1.com
HOST: www:
                                              Flashback    DNS resp.
                                              delay        selection
                                              (x100us)     counters
                                              TCP  APP     Count (%)
*    10.10.10.200: dns v-ip    ACTIVE N-AM       9   19    0 (0%)
*       1.1.1.101: dns v-ip    ACTIVE N-AM       0    0    4 (100%)
```

Syntax: **show gslb dns zone**

Implementing the weighted site metric

You can configure the ServerIron ADX to distribute SLB traffic among GSLB sites based on weights configured for the sites. The weights determine the percentage of traffic each site will receive in comparison with other sites, which may or may not have weights.

NOTE
You cannot use the weighted site metric if the weighted IP metric is enabled.

You assign weights to GSLB sites. Each GSLB site may consist of one or more ServerIron ADXs, but the weight is applicable to the site as a whole.

The GSLB ServerIron ADX uses relative percentages in order to achieve 100% total weight distribution, as shown in Table 5 and Table 6. In Table 5, the total of the Configured weighted site metrics (second column) is 100. The last column shows that the GSLB ServerIron ADX distributes the traffic to the IP addresses exactly as configured. In this example, traffic distribution is straightforward because the total weight of all three GSLB sites equals 100.

TABLE 5 Example weighted site metric configuration

GSLB site	Configured weighted site metric	Relative weighted site metric
San Jose	50	50%
New York	30	30%
London	20	20%
Total	100	100%

Now consider the example in Table 6. In this example, the total of the Configured weighted site metrics (second column) does not equal 100. However, as illustrated in the last column, the GSLB ServerIron ADX uses relative percentages in order to achieve 100% total weight distribution.

TABLE 6 Example weighted site metric configuration

IP address	Configured weighted site metric	Relative weighted site metric
San Jose	15	33% (15/45 * 100)
New York	20	44% (20/45 * 100)
London	10	22% (10/45 * 100)
Total	45	100%

By default, the weighted site metric is disabled. When enabled, it is placed second in the GSLB algorithm, after the Health Check metric. You can change the metric order and enable or disable other metrics, although we do not recommend this. For more information, refer to “Changing the order of GSLB policy metrics” on page 37.

DNS response processing

When the weighted site metric is enabled, the GSLB ServerIron ADX selects an IP address belonging to a particular site to be the best IP address in the DNS reply to a client. The client subsequently makes an SLB request to that IP address.

Using the weighted site metric, the GSLB algorithm calculates a relative weight for each IP address and selects the IP address with the least relative weight. The GSLB ServerIron ADX uses the following criteria to calculate the relative weight of an IP address:

- The number of times the GSLB ServerIron ADX selected the IP address as the best IP address to reply to a client
- The number of eligible IP addresses to be evaluated by the weighted site metric, and the weights of sites to which they belong
- A calculated weight assigned to an IP address, based on the following criteria:
  - If the IP address is a real server, then the calculated weight is zero
  - If the IP address is a Virtual IP (VIP), the weight is calculated based on the site the VIP belongs to, the weight of the site, and the number of candidate VIPs belonging to the site and being evaluated by the weighted site metric

If an IP address has a relative weight of zero, or if an IP address belongs to a site that does not have an assigned weight, the IP address is not selected as the best IP address for a client. Note that all real servers have a relative weight of zero, as do VIPs that belong to sites with no assigned weights.

If two or more IP addresses have the same relative weight, or if all of the IP addresses have a relative weight of zero, all of the IP addresses with the same relative weight are passed on to the next step in the GSLB algorithm, where the process of selecting the best IP address continues.

Traffic distribution specifications

In general, DNS response selection counters are maintained per IP address, per domain name. For example, suppose you configure three GSLB sites with assigned weights. All three sites host the application *www.gslb.com* and sites New York and London also host ftp.gslb.com, as illustrated below.

www.gslb.com
VIP 1.1.1.1 belongs to San Jose with a weight of 50
VIP 1.1.1.2 belongs to New York with a weight of 30
VIP 1.1.1.3 belongs to London with a weight of 20

ftp.gslb.com
VIP 1.1.1.2 belongs to New York with a weight of 30
VIP 1.1.1.3 belongs to London with a weight of 20

Suppose that 10 DNS requests are made to *www.gslb.com*. By viewing the selection counters (using the **show gslb dns zone** command), you would see that San Jose is selected 5 times (50%), New York is selected 3 times (30%), and London is selected 2 times (20%).

Now suppose that 5 DNS requests are made to ftp.gslb.com. In this case, New York receives 3 requests (60%), and London receives 2 requests (40%). This is because counters are maintained per IP address per domain name.

If you consider the total site traffic for both applications, the traffic distribution is as follows: San Jose = 5 (33%); New York = 6 (40%); and London = 4 (26%). The GSLB ServerIron ADX evaluates the results of the weighted metrics with respect to a specific domain name, not an IP address alone.

Configuring weighted site metrics

To configure weighted site metrics, complete the following tasks.

1. Enable the weighted site metric.
2. Select the site for which to apply weights.
3. Configure a weight for the site.

For example, enter commands such as the following:

```
ServerIronADX(config-gslb-policy)# weighted-site
ServerIronADX(config-gslb-policy)# gslb site SanJose
ServerIronADX(config-gslb-site-SanJose)# weight 50
```

Syntax: [no] weighted-site

Syntax: gslb site <*site name*>

The <*site name*> can have a maximum of 16 characters.

Syntax: weight <*weight*>

The <*weight*> is a value from 0 to 100. The default value is 0.

Displaying results of traffic distribution for Weighted Sites

To view the results of traffic distribution after configuring weighted site metrics, enter the following command.

```
ServerIronADX(config)# show gslb traffic site

SITE: local                             Weight: 50
        * a.b.c
          DNS Requests: 36
                ServerIronADX VIP                 Selection (%)
                ==                  ===                 =============
                1.1.1.1             1.1.1.181           9 (25 %)
                1.1.1.1             1.1.1.180           9 (25 %)
          Site Selection for Domain: 18 (50 %)
        * b.b.c
          DNS Requests: 0
                ServerIronADX VIP                 Selection (%)
                ==                  ===                 =============
                1.1.1.1             1.1.1.121           0 (0 %)
          Site Selection for Domain: 0 (0 %)

SITE: TWO                               Weight: 50
        * a.b.c
          DNS Requests: 36
                ServerIronADX VIP                 Selection (%)
                ==                  ===                 =============
                1.1.1.2             1.1.1.182           18 (50 %)
          Site Selection for Domain: 18 (50 %)
        * b.b.c
          DNS Requests: 0
                ServerIronADX VIP                 Selection (%)
                ==                  ===                 =============
                1.1.1.2             1.1.1.122           0 (0 %)
          Site Selection for Domain: 0 (0 %)
```

The first example shows the first two sites.

Syntax: **show gslb traffic site**

This command shows the domains hosted by each site. For each domain name, it shows how much traffic was sent to each ServerIron ADX in that site, and the total percentage of traffic sent to the site.

The second example shows the third site.

```
SITE: THREE

        * a.b.c
          DNS Requests: 36

                ServerIronADX VIP                 Selection (%)
                ==                  ===                 =============
                1.1.1.3             1.1.1.183           0 (0 %)
          Site Selection for Domain: 0 (0 %)

        * b.b.c
          DNS Requests: 0

                ServerIronADX VIP                 Selection (%)
                ==                  ===                 =============
                1.1.1.3             1.1.1.123           0 (0 %)
          Site Selection for Domain: 0 (0 %)
```

In the above examples, there are two hosts; a (HTTP) and b (FTP) which belong to the zone b.c. There are three sites as listed below:

- Local (weight: 50; ServerIron ADX: 1.1.1.1; VIPs: 1.1.1.180 (HTTP), 1.1.1.181 (HTTP), 1.1.1.121 (FTP)
- TWO (weight: 50; ServerIron ADX: 1.1.1.2; VIPs: 1.1.1.182 (HTTP), 1.1.1.122 (FTP))
- THREE (weight: 0; ServerIron ADX: 1.1.1.3; VIPs: 1.1.1.183 (HTTP), 1.1.1.123 (FTP))

The IP resolution for the domain names is as follows:

- a.b.c.: 1.1.1.180; 1.1.1.181; 1.1.1.182
- b.b.c.: 1.1.1.121; 1.1.1.122

After making 36 requests for domain "a.b.c.", the distribution was:

- Site Local got 18 requests (VIP 1.1.1.180 received 9 and VIP 1.1.1.181 received 9)
- Site TWO got 18 requests (VIP 1.1.1.182 received all 18)
- Site THREE did not receive any requests because its weight is zero

Implementing the active bindings metric

You can configure a ServerIron ADX to prefer an IP address with the highest number of active bindings.

Active bindings are a measure of the number of active real servers bound to a Virtual IP address (VIP) residing on a GSLB site. The GSLB ServerIron ADX uses the active bindings metric to select the best IP address for the client.   The VIP with the highest number of active bindings is the IP address preferred by the active bindings metric.

In order to implement the active bindings metric, the GSLB ServerIron ADX processes information it receives from an agent. For each VIP address on the agent ServerIron ADX, the agent reports the following information to the GSLB ServerIron ADX:

- The virtual ports configured
- The number of active real servers bound to the virtual port

For each VIP of interest, the GSLB ServerIron ADX stores the number of active bindings for the respective application port.

If the agent is running a software image that does not support the active bindings metric, it does not report any information specific to the active bindings metric. In this case, the default active bindings value for each VIP residing on that site is 1 or 0, depending on the health status of the VIP. If the VIP is active, the value is 1. If the VIP is not active, it is 0.

By default, the active bindings metric is disabled. When enabled, it is placed after the Num-Session metric in the GSLB algorithm. You can change the metric order or enable or disable other metrics, although we do not recommend this.

DNS response processing

When the active bindings metric is enabled, the GSLB ServerIron ADX evaluates each IP address in the DNS reply from the server, and selects the IP address with the highest number of active bindings. The client subsequently makes an SLB request to that IP address.

Active bindings are calculated as follows:

- If the IP address is a VIP residing on a remote site that supports active bindings, then the number of active bindings equals the number of active real servers bound for application ports.
- If the IP address is a VIP residing on a remote site that is running older versions of the GSLB agent software, and consequently does not support the active bindings metric, then the number of active bindings for the IP address is 1 or 0, depending on the health of the VIP.
- If the IP address is a real server, then the number of active bindings for the IP address is 1 or 0, depending on the health of the real server.

If all IPs or VIPs have zero active bindings, or if all IPs or VIPs have the same number of active bindings, the GSLB ServerIron ADX passes them on to the next step in the GSLB algorithm, where the process of selecting the best IP address continues. Likewise, if two or more IP addresses have the highest maximum value of active bindings, the GSLB ServerIron ADX passes them on to the next step in the GSLB algorithm.

Enabling active bindings

Active bindings are a measure of the number of active real servers bound to a Virtual IP address (VIP) residing on a GSLB site. The GSLB ServerIron ADX uses the active bindings metric to select the best IP address for the client. The VIP with the highest number of active bindings is the IP address preferred by the active bindings metric.

To configure the active bindings metric, enter the following command.

```
ServerIronADX(config-gslb-policy)# active-bindings
```

Syntax: [no] active-bindings

Displaying active binding information

To view active bindings for each IP address, enter the following command.

```
ServerIronADX# show gslb dns detail
```

Syntax: show gslb dns zone

Refer to "Displaying the results of traffic distribution for Weighted IPs" on page 42 for an example screen display.

GSLB active bindings enhancements

The following features have been added to GSLB active bindings:

- Weighed active bindings
- Minimum active bindings
- Tracking an application port for active bindings

Configuring weighted active bindings

Weighted Active Bindings allows you to configure the GSLB ServerIron ADX to direct requests to domain VIPs in proportion to their active bindings. For example, if VIP-1 has 2 active bindings and VIP-2 has 1 active binding, you can configure the GSLB ServerIron ADX to direct two-thirds of the client requests to VIP-1 and one-third of the client requests to VIP-2.

To enable weighted active bindings for the global GSLB policy, first enable the active bindings using the existing **active-bindings** CLI command, then configure the following additional command.

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# weighted-selection
ServerIronADX(config-gslb-policy)# end
ServerIronADX#
```

To enable weighted active bindings for the host level policy, first enable the active bindings using the existing **active-bindings** CLI command, then configure the following additional command.

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb-host-policy abc
ServerIronADX(config-gslb-host-policy-abc)# weighted-selection
ServerIronADX(config-gslb-host-policy-abc)# end
ServerIronADX#
```

Using minimum active bindings

You can configure the GSLB ServerIron ADX to use the minimum active bindings among all application ports if multiple application ports are associated with a domain. For example, if application ports http and ftp are configured for *www.companynet.com*, you may need the active bindings count for the VIPs to be based on the minimum of the active bindings for these two application ports. You can configure the GSLB ServerIron ADX to use minimum bindings as follows.

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb dns zone companynet.com
ServerIronADX(config-gslb-dns-companynet.com)# host-info www http
ServerIronADX(config-gslb-dns-companynet.com)# host-info www ssl
ServerIronADX(config-gslb-dns-companynet.com)# host-info www min-bindings
ServerIronADX(config-gslb-dns-companynet.com)# end
```

Tracking an application port for active bindings

You can configure the GSLB ServerIron ADX to track a particular application port for active bindings if multiple application ports are associated with a domain. For example, if application ports HTTP and SSL are configured for *www.companynet.com*, you may need the active bindings count for the VIPs to be based only on the active bindings for the HTTP port but not the SSL port. You can configure the GSLB ServerIron ADX to track active bindings for the http port only as follows.

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb dns zone company.com
ServerIronADX(config-gslb-dns-company.com)# host-info www http
ServerIronADX(config-gslb-dns-company.com)# host-info www ssl
ServerIronADX(config-gslb-dns-company.com)# host-info www http track-port
ServerIronADX(config-gslb-dns-company.com)# end
```

Configuring connection load parameters

A GSLB site's **connection load** is the average number of new connections per second on the site, over a given number of intervals. When you enable this GSLB metric, all potential candidates are compared against a predefined load limit. All sites that have fewer average connections than the threshold are selected and passed to the next comparison metric.

The connection load metric is disabled by default but is enabled (added to the GSLB policy) when you configure the metric.

You can configure the following parameters:

- Site connection limit
- Sampling intervals and sample rate
- Interval weights
- Comparison order in the GSLB policy

  When the connection load metric is enabled, by default the metric is used after the geographic location metric but before the session capacity metric. You can change the order in which the metrics are applied.

To configure the connection limit metric, perform the following tasks on the ServerIron ADX that is the GSLB controller. You do not need to perform any tasks on the site ServerIron ADXs. All configuration for the metric takes place on the controller.

- Specify the site connection limit. Specifying the site connection limit also enables the metric in the GSLB policy.
- **Optional**: Change the sampling intervals and sample rate.
- **Optional:** Change the relative weights of the sampling intervals.
- **Optional**: Change the position of the metric in the GSLB policy. By default, the metric comes after comparison of geographic locations and before comparison of session capacities.

Specifying the site connection limit

The site connection limit is the maximum number of new connections per second a site can have without being disqualified by the GSLB policy. During site comparison, when the GSLB policy is comparing otherwise equal sites based on the connection load metric, the policy disqualifies a site if its average number of new connections is higher than the specified connection limit.

The same connection limit applies to all sites. You can specify from 1 to as high a value as you need. There is no default. When you specify a value, the connection load metric is enabled (added to the GSLB policy).

This is the only parameter that you are required to set for the metric. The other parameters have default values.

To specify the site connection limit and enable the connection limit metric, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# connection-load limit 500
```

This command sets the site connection limit to 500 connections. During site comparison, the GSLB policy discards sites that have an average load of new connections that is higher than the amount you specify. All other sites are passed to the next GSLB policy metric as potential candidates.

Syntax: [no] connection-load limit <*average-load*>

You can specify from 1 to as high a value as you need. There is no default. You must specify a connection limit to enable the connection limit metric.

Changing the sampling intervals and sample rate

The sampling interval is the number of data samples the GSLB controller averages together to calculate a site's connection load. The sample rate is the number of seconds between intervals.

By default, each GSLB site takes five samples, at 5-second intervals. Using the default sampling interval and sample rate, the site takes samples after 5 seconds, 10 seconds, 15 seconds, 20 seconds, and 25 seconds.

The number of new connections the site has at each of the five intervals is averaged together. This average value is the one the GSLB controller uses for the comparison:

- You can specify from 1-8 sampling intervals. The default is 5.
- You can specify from 5-60 seconds for the sample rate. The default is 5 seconds.

At any given time, the average connection load for a site is the average of the latest full set of data samples. For example, if the sampling interval is 5, then the average load is the average of the five most recent samples.

NOTE
The accuracy of the average is affected by the initial sampling rate. For example, if the sampling rate is 5 seconds, the average at the seventh second will consist of the average for the first through fifth seconds, rather an average for the second through seventh seconds.

By default, the site ServerIron ADX samples the load of new connections every five seconds and stores the average connection load for five intervals: the average loads at the previous 5, 10, 15, 20, and 25 seconds.

You can change the sampling interval and sample rate. Enter a command such as the following at the GSLB policy level of the CLI.

```
ServerIronADX(config-gslb-policy)# connection-load intervals 6 5
```

This command changes the number of sampling intervals from 5 to 6 but leaves the sample rate set to 5 seconds. At any given time, the site ServerIron ADX will have the average load for six intervals, for the previous 5, 10, 15, 20, 25, and 30 seconds. The average connection load will be calculated based on these six samples.

Syntax: [no] connection-load intervals <*num-intervals*> <*sampling-rate*>

The <*num-intervals*> parameter specifies the number of samples you want the site ServerIron ADX to collect and average together. You can specify 1-8 intervals. The default is 5.

The <*sampling-rate*> parameter specifies the number of seconds between each sample. You can specify 1-60 seconds. The default is 5 seconds.

Changing the sample interval weight

The interval weights are the relative weights of each data sample within a set of sampling intervals. When the data samples are averaged together, the relative weights of the samples can affect the outcome. You can adjust the load calculation formula by changing the weights of the intervals, so that some intervals are counted more heavily towards the average than other intervals. You can even eliminate the effect of an interval by setting its weight to 0.

For example, if a sampling interval contains six data samples and you assign higher weights to the third and fourth samples than to the others, the third and fourth samples play a larger role when the average connection load is calculated.

The default weight for each interval is 1. You can individually change the weight to a value from 0-10. If you set an interval's weight to 0, that interval is not included when the intervals are averaged together.

By default, the site ServerIron ADX weighs each data sample equally when calculating the connection average for the GSLB policy. The weight of each interval is 1 by default.

You can change the weights to give more emphasis to some intervals and less emphasis to others. For example, if you are using five intervals, all five have equal influence on the average load calculated by the GSLB policy. If you want to give more emphasis to the third interval, you can give the third interval a higher weight than the other intervals. To ignore an interval when calculating the average, assign the weight 0 (zero) to the interval.

To change sample weights, enter a command such as the following at the GSLB policy level of the CLI.

```
ServerIronADX(config-gslb-policy)# connection-load weights 1 1 3 1 1
```

This command gives more weight to the third sampling interval than to the other intervals, while including all intervals in the calculation of the average connection load.

Syntax: [no] connection-load weights <*weight1*> [<*weight2*>...<*weight8*>]

The <*weight*> parameters specify the weights. You can specify from 0-10. If you enter 0, the interval is not included when calculating the average load. Enter the weights in the same order as the sampling intervals.

You do not need to enter weight values for all the intervals once you enter the last non-zero weight. For example, if you want to set the weight for interval three to 1 but use 0 for the weights of all the other intervals, you can enter the following command.

```
ServerIronADX(config-gslb-policy)# connection-load weights 0 0 1
```

When this command is entered, the weights for the fourth interval and higher are set to 0.

Changing the session-table capacity threshold and tolerance values

You can change the following parameters associated with the session-table metrics:

- **Session capacity threshold**: Specifies how close to the maximum session capacity the site ServerIron ADX (remote ServerIron ADX) can be and still be eligible as the best site for the client. This mechanism provides a way to shift load away from a site before the site becomes congested. The default value for the threshold is 90%. Thus a site ServerIron ADX is eligible to be the best site only if its session utilization is below 90%.
- **Available session capacity tolerance**: Specifies the percentage by which the number of available sessions on the site ServerIron ADX can differ from the number of available sessions on another site ServerIron ADX and still be considered an equally good site.

You can change these parameters on an individual basis.

To change the session-table capacity metric, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# capacity threshold 99
```

Syntax: [no] capacity threshold <*num*>

The <*num*> parameter specifies the maximum percentage of a site ServerIron ADX's session table that can be in use. If the ServerIron ADX's session table utilization if greater than the specified percentage, the GSLB ServerIron ADX prefers other sites over this site. You can specify a percentage from 0-100. The default is 90.

To change the session-table tolerance metric, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# num-session tolerance 20
```

Syntax: [no] num-session tolerance <*num*>

The <*num*> parameter specifies the maximum percentage by which the session table utilization on ServerIron ADXs at different sites can differ without the GSLB ServerIron ADX selecting one over the other based on this metric. You can specify a tolerance from 0-100. The default is 10.

Changing the FlashBack tolerance values

You can modify the following FlashBack parameters:

- Application tolerance
- TCP tolerance

The GSLB ServerIron ADX uses a tolerance value when comparing the FlashBack speeds of different sites. The tolerance value specifies the percentage by which the FlashBack speeds of the two sites must differ in order for the ServerIron ADX to choose one over the other. The default FlashBack tolerance is 10%. Thus, if the FlashBack speeds of two sites are within 10% of one another, the ServerIron ADX considers the sites to be equal. However, if the speeds differ by more than 10%, the ServerIron ADX prefers the site with the lower FlashBack speed.

FlashBack speeds are measured at Layer 4 for all TCP/UDP ports. For the application ports known to the ServerIron ADX, the FlashBack speed of the application is also measured.

When the ServerIron ADX compares the FlashBack speeds, it compares the Layer 7 (application-level) FlashBack speeds first, if applicable. If the application has a Layer 7 health check and if the FlashBack speeds are not equal, the ServerIron ADX is through comparing the FlashBack speeds. However, if only the Layer 4 health check applies to the application, or if further tie-breaking is needed, the ServerIron ADX then compares the Layer 4 FlashBack speeds.

To change the tolerances for the response times of TCP and application health checks, when used as a metric for selecting a site, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# flashback application tolerance 30
ServerIronADX(config-gslb-policy)# flashback tcp tolerance 50
```

Syntax: [no] flashback application | tcp tolerance <*num*>

The **application | tcp** parameter specifies whether you are modifying the tolerance for the Layer 4 TCP health check or the Layer 7 application health checks. You can change one or both and the values do not need to be the same. For each, you can specify from 0-100. The default for each is 10.

Modifying round-trip time values

The Round-trip time (RTT) is the amount of time that passes between when the remote site receives a TCP connection (sends a TCP SYN) from the client and when the remote site receives the client's acknowledgment of the connection request (sends a TCP ACK). A site ServerIron ADX sends RTT data to the GSLB ServerIron ADX every five seconds.

You can modify RTT parameters to change processing of the RTT information reported by the GSLB and remote site ServerIron ADXs. You can change the following parameters, on an individual basis:

- **RTT cache interval:** The site ServerIron ADXs use the GSLB protocol to send RTT information to the GSLB ServerIron ADX. The GSLB ServerIron ADX stores this information in a cache. The GSLB ServerIron ADX uses the entries in the cache when using the RTT metric to evaluate IP addresses in a DNS reply. Entries in the cache age out if they remain unused. The default aging interval for RTT cache entries is 120 seconds. You can change the interval to a value from 10-1,000,000 seconds (about 11-1/2 days).
- **RTT cache prefix:** The entries in the RTT cache include IP address information for the clients. To avoid overflowing the cache, cache entries are aggregated based on the IP information. For example, if the GSLB ServerIron ADX receives RTT information for clients at 192.21.4.69 and 192.21.4.18, and the cache prefix is 31 bits, both addresses go in as separate entries. However, if the prefix is 16 bits, the GSLB ServerIron ADX aggregates the addresses. In this case, only one entry, 192.21.x.x goes in the cache. The default number of bits in the prefix is 20. You can specify a value from 1-31.
- **RTT tolerance**: When the GSLB ServerIron ADX compares two site IP addresses based on RTT, the GSLB ServerIron ADX favors one site over the other only if the difference between the RTT values is greater than the specified percentage. This percentage is the RTT tolerance. You can set the RTT tolerance to a value from
  0-100. The default is 10%.
- **RTT explore percentage:** Site ServerIron ADXs send RTT information only for the sessions that clients open with them. These are clients referred to the site ServerIron ADX by the GSLB ServerIron ADX. If the metrics that come before this one (based on the GSLB policy order) do not select a "best" site, the ServerIron ADX selects a site based on RTT.

  Since the only RTT information received by the GSLB ServerIron ADX comes from the site ServerIron ADXs to which the GSLB ServerIron ADX has referred clients, it is possible for the GSLB ServerIron ADX to continually bias its selection toward the first site ServerIron ADX that sent RTT information. To prevent this from occurring, the GSLB ServerIron ADX intentionally ignores the RTT metric for a specified percentage of the requests from a given client network. You can specify an RTT explore percentage from 0-100. The default is 5. By default, the GSLB ServerIron ADX ignores the RTT for 5% of the client requests from a given network.

You also can add static RTT prefix cache entries.

Changing the RTT cache interval

You can change the round trip time (RTT) cache interval, which specifies how often the site ServerIron ADXs use the GSLB protocol to send RTT information to the GSLB ServerIron ADX. The GSLB ServerIron ADX stores this information in a cache. The GSLB ServerIron ADX uses the entries in the cache when using the RTT metric to evaluate IP addresses in a DNS reply.

To change the RTT cache interval from 10 seconds to 30 seconds, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# round-trip-time cache-interval 30
```

Syntax: [no] round-trip-time cache-interval <*num*>

The <*num*> parameter specifies the aging interval and can be from 10-1,000,000 seconds (about 11-1/2 days). The default is 120 seconds.

Changing the RTT cache prefix

You can change the RTT cache prefix, which specifies the level of aggregation that occurs in the GSLB ServerIron ADX's RTT cache.

The entries in the RTT cache include IP address information for the clients. To avoid overflowing the cache, cache entries are aggregated based on the IP information. For example, if the GSLB ServerIron ADX receives RTT information for clients at 192.21.4.69 and 192.21.4.18, and the cache prefix is 31 bits, both addresses go in as separate entries. However, if the prefix is 16 bits, the GSLB ServerIron ADX aggregates the addresses. In this case, only one entry, 192.21.x.x goes in the cache.

To change the RTT cache prefix from 20 bits to 16 bits, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# round-trip-time cache-prefix 16
```

Syntax: [no] round-trip-time cache-prefix <*num*>

The <*num*> parameter specifies the number of significant bits in the prefix and can be from 1-32. The default is 20.

Changing the RTT tolerance

To change the RTT tolerance from 10% to 70%, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# round-trip-time tolerance 70
```

Syntax: [no] round-trip-time tolerance <*num*>

The <*num*> parameter specifies the percentage above which the RTTs of two sites must differ for the GSLB ServerIron ADX to favor one site over the other based on the RTT. You can specify a value from 0-100. The default is 10%.

Change the RTT explore percentage

You can change the RTT explore percentage, which prevents the GSLB ServerIron ADX from unfairly biasing selection of the best site based on previous RTT responses.

Site ServerIron ADXs send RTT information only for the sessions that clients open with them. These are clients referred to the site ServerIron ADX by the GSLB ServerIron ADX. If the metrics that come before this one (based on the GSLB policy order) do not select a "best" site, the ServerIron ADX selects a site based on RTT.

Since the only RTT information received by the GSLB ServerIron ADX comes from the site ServerIron ADXs to which the GSLB ServerIron ADX has referred clients, it is possible for the GSLB ServerIron ADX to continually bias its selection toward the first site ServerIron ADX that sent RTT information. To prevent this from occurring, the GSLB ServerIron ADX intentionally ignores the RTT metric for a specified percentage of the requests from a given client network. You can specify an RTT explore percentage from 0-100. The default is 5. By default, the GSLB ServerIron ADX ignores the RTT for 5% of the client requests from a given network.

To change the RTT explore percentage, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# round-trip-time explore-percentage 10
```

The command in this example changes the RTT explore percentage from 5% to 10%.

Syntax: [no] **round-trip-time explore-percentage** *<num>*

The *<num>* parameter specifies the explore percentage and can be from 0-100. The default is 5.

Adding static prefix cache entries

The GSLB ServerIron ADX maintains a cache of round-trip time (RTT) information received from the site ServerIron ADXs through the GSLB protocol. The RTT is the amount of time that passes between when a remote site initiates a TCP connection from the client and when the remote site receives the client's acknowledgment of the connection request. Each site ServerIron ADX sends RTT information to the GSLB ServerIron ADX at one-second intervals.

The GSLB ServerIron ADX uses the RTT information in the prefix cache when evaluating a site using the GSLB policy. Thus, the cache entry provides the RTT information used for the RTT metric during evaluation of the GSLB policy.

When the GSLB ServerIron ADX receives RTT information from a site ServerIron ADX, the IP address of the client is compared to the prefixes in the cache. If the address fits within a network in one of the prefixes, the GSLB ServerIron ADX stores the RTT information for that site under the prefix entry. If the client address is within more than one prefix entry, the GSLB ServerIron ADX selects the entry with the longer prefix (the more exact match).

The GSLB ServerIron ADX makes a dynamic entry in the prefix cache of the length specified by the cache prefix the first time the ServerIron ADX processes a DNS query or response from that prefix. After that, each time the GSLB ServerIron ADX receives a subsequent DNS query from within that prefix, the ServerIron ADX resets the aging timer for the cache prefix entry. If a dynamic entry is not refreshed by subsequent queries, the entry ages out.

You can manually add static prefix information to the cache. For example, you can add static cache entries with longer prefix information than the dynamic cache entries to ensure that RTT information is stored under the static entries instead of dynamic cache entries with shorter prefixes. This is useful when you want to ensure that certain prefixes are always present in the cache regardless of how often the GSLB ServerIron ADX receives RTT data for them. Static prefixes do not age out.

NOTE
The GSLB ServerIron ADX uses the most exact match when more than one prefix entry can apply to the same site address. To ensure that the GSLB ServerIron ADX uses a static entry instead of certain dynamic entries for a given address, make sure prefix of the static entry is longer than the prefix for dynamic entries.

NOTE
Since RTT information is stored under individual domain names that are queried, the RTT information reported from remote ServerIron ADXs are not recorded under the static records until the GSLB ServerIron ADX receives the first DNS query or response.

To add a static prefix cache entry, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# static-prefix 61.1.1.1/20
```

Syntax: **static-prefix** *<ip-addr>*/*<prefix-length>*

The *<ip-addr>* specifies the address of the cache entry. This is not necessarily the address of a remote site. The address you specify here is combined with the prefix length to result in a network prefix (network portion of an IP address). The prefix length can be from 1-31.

NOTE
The prefix length 0 is not applicable to this feature and is ignored by the software.

You can enter more than one prefix on the same command line. Separate each prefix with a space. You can configure up to 250 static prefixes on a ServerIron ADX.

The command in this example configures an entry for address 61.1.1.1 with a prefix of 20 bits. (Due to the prefix length, the value actually stored in the cache is 61.1.0.0.20.) When the GSLB ServerIron ADX receives RTT information for an address within the specified prefix, the GSLB ServerIron ADX stores the information in the static prefix entry configured above, instead of creating a dynamic entry.

Enabling default geographic location

The **use-default-location** command enables you to ensure that the geographic policy metric is used to load balance client requests even if the client prefix cache maintained by the GSLB ServerIron ADX is full.

By default, the GSLB ServerIron ADX ignores the default location of new client requests if its client prefix cache if full. Whenever the GSLB ServerIron ADX cannot create a new entry in the client prefix cache because it has already exceeded the limit, it ignores the geographic policy metric and falls to the next metric in the GSLB policy.

If the **use-default-location** command is configured for either the global GSLB policy or the host-level GSLB policy, the ServerIron ADX uses the default location of the client and the geographic policy metric when determining how to distribute the client's request.

To ensure that the geographic policy metric is used, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# use-default-location
```

The default location of the client corresponds to the default location configured on the GSLB controller. If no default location is configured on the GSLB controller, then n-america is assigned by default. For more information, see "Specifying GSLB controller locations" on page 21

Secure GSLB

Secure GSLB uses industry standard algorithms and mechanisms to authenticate and encrypt Global Server Load Balancing (GSLB) protocol communication between the GSLB controller and site ServerIron ADXs.

GSLB controllers and site ServerIron ADXs communicate and exchange information using the GSLB protocol. This protocol comprises a set of messages for exchanging information, and each message type has a unique format.

Secure GSLB communication provides the following benefits:

- **Peer authentication** — Each network device must be authenticated before it can connect to the GSLB network. This check ensures that any peer a GSLB device communicates with is the legitimate peer. Peer authentication is provided by using the Rivest-Shamir-Adleman (RSA) public key technology. The key length is 1024 bits.
- **Data Encryption** — Converts plaintext into cipher text (encrypted data). Only the designated receiver can decrypt and retrieve the information. Encryption of the GSLB protocol message data will deny unauthorized access to the GSLB protocol data. All GSLB protocol messages between the controller and site ServerIron ADX are encrypted using the Blowfish Cipher Block Chaining (CBC) algorithm. The key length is 256 bits (standard 16 rounds).
- **Data integrity** — Reassures the recipient the message has not been altered after it was generated and transmitted by a legitimate source. Data integrity is ensured by using Hashed Message Authentication Codes (HMAC) with SHA1. The key length is 20 bytes. The digest length is 20 bytes.

  A MAC is included with each GSLB protocol packet. The MAC is computed using the authentication key, packet sequence number, and the contents of the packet:

  mac = MAC(key, sequence-number || unencrypted-packet)

  The unencrypted packet refers to the entire packet without a MAC. The sequence number is a 32-bit implicit packet sequence number. This number is initialized to zero for the first packet, and it is incremented for every GSLB protocol packet sent thereafter.

  The message authentication key is negotiated during authentication phase as described in the section "Initial session key generation" on page 57.
- **Data authentication** — Guarantees that the sender of the data is the legitimate peer. An authentication-session key is used to perform a hash between the peers that have already been authenticated. Only the two peers can generate the hash based on the key.

  Each MAC hash is generated using the negotiated authentication key. This key is shared between the two peers. Therefore, a message received with the correct MAC hash authenticates the peer because only the sender and the receiver have knowledge of the authentication key.
- **Protection** — Against replay and "man-in-the-middle" attacks.
- **Dynamic session key generation** — Makes it difficult for an intruder to decipher session keys, by regenerating keys periodically or randomly.

Initial session key generation

Once the initial authentication is completed, the GSLB controller generates two session keys:

- Encryption key
- Authentication key

These keys are randomly generated. The secure random generator from the RSA toolkit is used for random number generation.

When the GSLB controller sends the session keys to the site, the keys are first encrypted with the local private key followed by public key of the peer. An SHA-1 digest of the keys is also attached to the message. In effect, both authentication and integrity are provided.

On receiving these encrypted passwords from the GSLB controller, the site ServerIron ADX decrypts the encryption key and authentication key using its private key and peer public key and verifies the SHA-1 hash is same as received. RSA decryption technology is used for this purpose.

RSA challenge dialogue

Once the initial peer authentication is complete, there is a challenge response dialogue between the two ServerIron ADXs as follows.

From GSLB controller to site ServerIron ADX:

- GSLB controller uses the site ServerIron ADX public key to encrypt a random sequence of bytes.
- The GSLB controller sends these encrypted bytes to the site ServerIron ADX.
- The site ServerIron ADX uses its private key to decrypt the bytes.
- The site ServerIron ADX sends the decrypted bytes back to the GSLB controller.
- The GSLB controller compares the decrypted bytes to the original bytes it sent to the site ServerIron ADX.

If the two sets of bytes match, it means the site ServerIron ADX's private key corresponds to an authorized public key, and the site ServerIron ADX is authenticated.

From site ServerIron ADX to GSLB controller:

- Site ServerIron ADX uses the public key of the GSLB controller to encrypt a random sequence of bytes.
- The site ServerIron ADX sends these encrypted bytes to the GSLB controller.
- The GSLB controller uses its private key to decrypt the bytes.
- The GSLB controller sends the decrypted bytes back to the site ServerIron ADX.
- The site ServerIron ADX compares the decrypted bytes to the original bytes it sent to the GSLB controller.

If the two sets of bytes match, it means that the GSLB controller's private key corresponds to an authorized public key, and the GSLB controller is authenticated.

NOTE
The above two exchanges are independent of each other. The decrypted bytes are sent back using TCP/IP protocol.

GSLB message content randomization

An implicit sequence number along with changing GSLB protocol data ensures the packet data changes from packet to packet resulting in a substantially different MAC for each packet.

Although, few of the GSLB protocol packets may have a relatively constant pattern. Therefore, the system introduces a random 8-bit data value in each packet. This value changes for each GSLB protocol packet resulting in a substantially different hash digest for every packet.

Configuring secure GSLB

The minimum required configuration for Secure GSLB includes the following tasks:

- Configure secure communication on the controller.
- Generate RSA Key Pair
- Exchange the Public Keys

Configuring secure-communication on the controller

On the GSLB controller, to enable the secure protocol instead of the standard one, enter commands such as the following:

```
SLB-Ctrl-ServerIronADX(config)# gslb site sfo
SLB-Ctrl-ServerIronADX(config-gslb-site-sfo)# si slb-1 100.1.1.3
secure-communication
```

Syntax: si <*si-name*> <*si-ip-address*> secure-communication

The GSLB site ServerIron ADX will automatically understand the secure protocol. There is no CLI command required to enable the feature on the site.

If you want the GSLB site ServerIron ADX to accept only the secure protocol and reject the standard GSLB connection request, then enter the following command on the site ServerIron ADX.

```
SLB-Site-ServerIronADX(config)# gslb auth-encrypt-communication secure-only
```

Syntax: gslb auth-encrypt-communication secure-only

Generating RSA key pair

Before authentication can proceed, each ServerIron ADX that is secure GSLB enabled must generate a static RSA public/private key pair for itself. The private key is used to prove the identity of the local device. It never leaves the system. In comparison, the public key is sent to the remote peer. The peer then uses that key to decrypt data.

The private key and public key compensate each other.

Private(Public(A)) = A and
Public(Private(A)) = A

You can refer to either operation as encryption and the other decryption. Many engineers refer to the public key operation as encryption, and call the private key operation decryption.

Use the **crypto key generate rsa** command on both the controller and site ServerIron ADXs to generate a random RSA public/private key pair. This key pair needs to be generated on each ServerIron ADX involved in the secure GSLB communication. Since the keys on each box are generated together, they are always in agreement.

Syntax: [no] crypto key generate rsa

Example

The following GSLB controller example assumes a minimum working GSLB configuration is already set up (refer to page 64).

```
SLB-Ctrl-ServerIronADX(config)# ip dns domain-name foo.com
SLB-Ctrl-ServerIronADX(config)# crypto key generate rsa
Generating rsa
keypair..................................................................done!
rsapublic_key"10243516320480114350385337927420684604699847215100737339140179784
0463596710017038795521320990076735951547998548950700124427622983729636247496044
8810297880244822925958194700326493941745541854086588315530748050102379348032059
7889011743490357195498301864347794398342179943239191530516416905654211931607212
87517491 chassis@foo.com"
rsa private_key "*************************"
```

```
ServerIron(config)#wr mem
.Write startup-config in progress.
..Write startup-config done.
ServerIron(config)#Saving SSH host keys process is ongoing. Please wait
.................................................................................
......Writing SSH host keys is done!
SLB-Ctrl-ServerIronADX(config)#^Z
SLB-Ctrl-ServerIronADX#reload
```

A **write mem** followed by a **reload** is required. Next, enter the **crypto key generate rsa** command on the site ServerIron ADX and **reload.**

Notice the public key is cleartext whereas the private key is not.

NOTE
The crypto RSA component calls the same key functions as SSH. Similar to the SSH implementation, the public and private keys for each ServerIron ADX are stored in its E2PROM. The private key cannot be seen or displayed using any CLI commands or any other user interface. Not even an administrator can gain access to the private key.

Exchanging public keys

Each ServerIron ADX must exchange public keys with each peer ServerIron ADX it needs to communicate with. This exchange allows the peers to authenticate before the GSLB communication starts.

The ServerIron ADX uses an out-of-band channel to deliver the fingerprint of the public key, which ensures the key comes from a trusted authority. To exchange public keys, the network administrator needs to telephone the peer site administrator to read out the fingerprint of the public key and verbally verify the keys match. SHA-1 is the algorithm used to generate the fingerprint.

The public key exchange sequence is illustrated below with an example. In the example, Bob (the site ServerIron ADX) and David (the controller ServerIron ADX) are two network administrators who want to exchange the public keys. For security reasons, We recommend that both administrators be locally logged into the console ports (not telnetted in) during this procedure.

1. (Optional) Both Bob and David issue the **gslb auth-encrypt-communication peer-pub-key-expire** <*timeout*> command before exchanging keys using **crypto key-exchange passive**. If the keys were exchanged first, a **one-time** usage would not take affect until the next exchange. Refer to "Selecting a peer public key management option" on page 62 for more options. If you do not set a **peer-pub-key-expire**, the default value is 180 seconds.

   ```
   SLB-Site-ServerIronADX(config)# gslb auth-encrypt-communication
   peer-pub-key-expire one-time
   ```

2. Bob enables a key exchange connection with the following command.

   ```
   SLB-Site-ServerIronADX(config)#crypto key-exchange passive
   Enter Control-c to abort if connection does not complete.
   Wait for connection from peer(enter 'y' or 'n'): y
   Waiting ....
   ```

   The command syntax is **crypto key-exchange passive** [<*decimal*>]. The <*decimal*> parameter specifies the TCP port used for the key exchange communication. If you use <*decimal*>, the value configured on both the sending side and receiving side must match.

NOTE
When you specify a TCP port for the key exchange communication, DO NOT use port 182, or the port that you configured for GSLB communication traffic. The default destination TCP port for key exchange is 56895.

To change default TCP port when doing public key exchange, enter a command such as the following:

```
ServerIronADX(config)# crypto key-exchange passive 111
```

3. David connects to Bob's device and send his RSA public key. The fingerprint of the key is displayed on David's screen.

```
SLB-Ctrl-ServerIronADX(config)#crypto key-exchange 100.1.1.1
Ctrl-ServerIronADX
Public key for Ctrl-ServerIronADX:
  Serial Number
  Fingerprint 7355edda 95906e7e f04e38a3 61f640fa c2e61fa7
```

The command syntax is crypto key-exchange <*IP address*> <*name*> [<*decimal*>].

The <*IP address*> parameter specifies peer IP address this device talks to. The <*name*> parameter specifies the host name of local device. The <*decimal*> parameter specifies TCP port used for the key exchange communication, such as the following:

```
ServerIronADX(config)# crypto key-exchange 100.1.1.1 test 111
```

4. Bob receives David's public key. The fingerprint is printed on Bob's screen. Both Bob and David read out the fingerprint and verify they match.

```
SLB-Site-ServerIronADX(config)#
Public key for Ctrl-ServerIronADX:
  Serial Number
  Fingerprint 7355edda 95906e7e f04e38a3 61f640fa c2e61fa7
Add this public key to the configuration?(enter 'y' or 'n'):
```

If they are the same, Bob answers `Y' to accept David's public key.

5. David waits for Bob to send his public key.

```
Wait for peer to send a key(enter 'y' or 'n'): y
Waiting ....
```

6. Bob sends back his public key.

```
Send peer a key in return(enter 'y' or 'n'): y
Public key for Site-ServerIronADX:
  Serial Number
  Fingerprint  92c8e6a2 cfe214e8 2645886f 2c7c6379 e0bfd96e
```

7. On David's device, Bob's fingerprint is displayed. Once again, both Bob and David read out the fingerprint to verify the key.

```
SLB-Ctrl-ServerIronADX(config)#
Public key for Site-ServerIronADX:
  Serial Number
  Fingerprint  92c8e6a2 cfe214e8 2645886f 2c7c6379 e0bfd96e
```

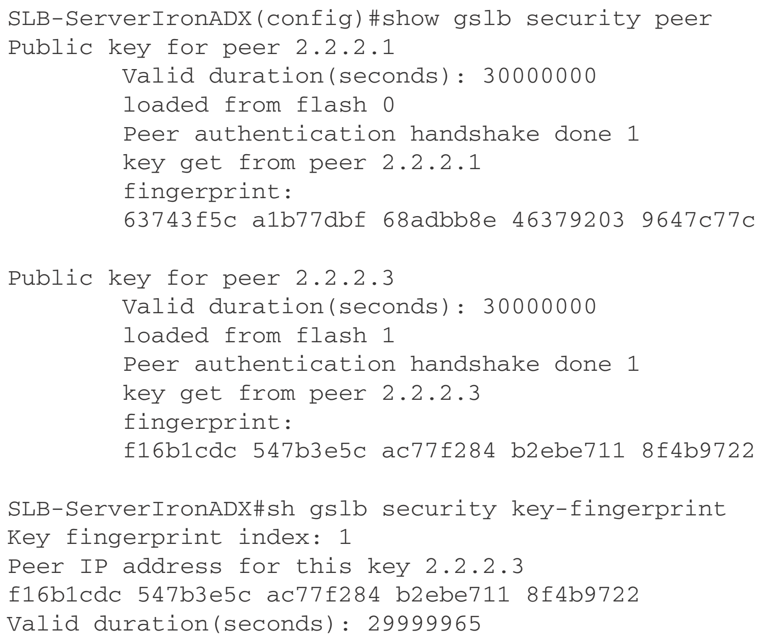
8. David accepts Bob's public key and adds it to his database. The key exchange is complete.

```
  Add this public key to the configuration?(enter 'y' or 'n'): y
```

9. After the key-exchange (fingerprint) takes place, the key must be saved on both the controller and site ServerIron ADX using the **crypto key-exchange save-peer-key** command. Notice there is an **erase-peer-key** option also.

```
SLB-Ctrl-ServerIronADX(config)#crypto key-exchange ?
  A.B.C.D           IP address of peer
  erase-peer-key    Erase peer public key in flash
  passive
  save-peer-key     Save peer public key into flash
SLB-Ctrl-ServerIronADX(config)#crypto key-exchange save-peer-key
```

To verify the communication state and public fingerprint key entry being exchanged, enter a command such as in the following:



```
SLB-ServerIronADX(config)#show gslb security peer
Public key for peer 2.2.2.1
        Valid duration(seconds): 30000000
        loaded from flash 0
        Peer authentication handshake done 1
        key get from peer 2.2.2.1
        fingerprint:
        63743f5c a1b77dbf 68adbb8e 46379203 9647c77c

Public key for peer 2.2.2.3
        Valid duration(seconds): 30000000
        loaded from flash 1
        Peer authentication handshake done 1
        key get from peer 2.2.2.3
        fingerprint:
        f16b1cdc 547b3e5c ac77f284 b2ebe711 8f4b9722

SLB-ServerIronADX#sh gslb security key-fingerprint
Key fingerprint index: 1
Peer IP address for this key 2.2.2.3
f16b1cdc 547b3e5c ac77f284 b2ebe711 8f4b9722
Valid duration(seconds): 29999965
```

Syntax: **show gslb security peer**

Syntax: **show gslb security key-fingerprint**

Selecting a peer public key management option

After the key exchange is completed, there are three key-management options provided to you.

Select the desired option based on the level of security required, balanced with an acceptable level of administration overhead for the key exchange.

To select the one-time option, enter the following command.

```
Secure-ServerIronADX(config)#gslb auth-encrypt-communication peer-pub-key-expire
one-time
```

If you do not set a **peer-pub-key-expire**, the default value is 180 seconds.

Syntax: **[no] gslb auth-encrypt-communication peer-pub-key-expire [one-time | never |** *<timeout>***]**

The **one-time** option configures the peer public keys for a **one-time** usage, which is the highest level of security. They expire after each TCP session to the peer device is disconnected. To set up a new connection between the devices to forward GSLB messages, you must redo the key exchange steps detailed previously. When you enable the **gslb auth-encrypt-communication secure-only** option on a site, the ServerIron ADX will communicate only with the controller that is Secure GSLB enabled.

Consider issuing the command **gslb auth-encrypt-communication peer-pub-key-expire one-time** before exchanging keys using **crypto key-exchange passive**. If you exchange the keys first, the **one-time** usage will not take affect until the next exchange.

The **never** option, after the initial public key exchange, configures the peer public keys to **never** automatically expire. They are assumed to be valid until and unless the administrators manually intervene and perform the public key exchange. The keys will be saved and reused for new TCP connections. Network administrators do not need to be involved after initial key exchange.

The <*timeout*> parameter configures the peer public keys to be valid for a specific duration of seconds independent of how many TCP connection setup and tear down events occur during this time. If the TCP connection is not established for the user-configured period of time, or if the connection to the peer is lost for this duration of time, these keys time out (expire). In this case, the key exchange and authentication procedure detailed earlier is required to set up a new connection.

Regenerating the session keys

To prevent the encryption key and authentication keys from being compromised, the system supports dynamic or manual session key regeneration.

Manually regenerating the session keys

To manually clear the session keys and force the regeneration of session keys, enter the following command.

```
Secure-GSLB-ServerIronADX# clear gslb session-keys
```

Syntax: clear gslb session-keys

Dynamically regenerating the session keys

The system dynamically regenerates the encryption and authentication keys (session keys) either at a specified regenerate-key-interval or at random.

The configure the system to dynamically regenerate the session keys at a specified interval, enter commands such as the following:

```
Secure-GSLB-ServerIronADX(config)# gslb site sfo
Secure-GSLB-ServerIronADX(config-gslb-site-sfo)# si slb-1 100.1.1.3
regenerate-key-interval 30
```

To configure the system to randomly decide when to regenerate the key within 1-30 minutes, enter commands such as the following:

```
Secure-GSLB-ServerIronADX(config)# gslb site sfo
Secure-GSLB-ServerIronADX(config-gslb-site-sfo)# si slb-1 100.1.1.3
regenerate-key-interval 30 random
```

Syntax: [no] si <*si-name*> <*si-ip-address*> **regenerate-key-interval** <*duration*> **[random]**

The <*si-name*> parameter specifies the name of the peer site ServerIron ADX to regenerate the session keys for.

The <*si-ip-address*> parameter specifies the IP address of the peer site ServerIron ADX.

The **regenerate-key-interval** <*duration*> parameter configures the ServerIron ADX to periodically regenerate session keys for the peer site ServerIron ADX. Each time a connection is set up, this key is regenerated and negotiated.

The <*duration*> specifies the duration in minutes after which new session keys will be regenerated.

The **random** option configures the controller to regenerate session keys for the peer site ServerIron ADX at a bounded random frequency.

When used with **random**, the <*duration*> parameter specifies the bound on the random key regeneration duration in minutes. The key will be randomly regenerated between 1 minute and the upper bound specified by the duration parameter.

Minimum GSLB configuration

Following is a sample minimum GSLB controller configuration for Secure GSLB. Note the **si secure-communication** command.

```
server real dns-rs 20.20.20.105
  port dns
  port dns one "brocade.com"
  port dns proxy
  port http
  port http url "HEAD /"
!
!
server virtual dns-vs 8.8.8.200
  port dns
  port http
  bind dns dns-rs dns
  bind http dns-rs http
!
gslb protocol
gslb sit brocade
  si si-1 2.2.2.1
  si si-2 2.2.2.3 secure-communication

gslb dns zone brocade.com
  host-info www http
```

Site persistence in GSLB using stickiness

Sticky GSLB enables the GSLB controller to return the same IP address if a client sends multiple DNS requests within a configurable period of time. This feature ensures the client is directed to the site that was previously visited.

For example, a business case for Sticky GSLB includes when user-specific content is stored at one site, such as a shopping cart. Being redirected to a site that no longer stores the content would result in a lost session.

To return the same IP address for a client that has sent requests previously, the GSLB controller must save the following information:

- Client IP address/prefix
- Domain name the client requested
- Selected IP address for the request

This information is saved in a session table when the Sticky GSLB feature is enabled, and the GSLB controller creates a sticky session for each client within the session table. Each session has a special user type and source port or destination port number to distinguish from other sessions.

When a new request enters the system, the GSLB controller searches for the client IP and domain name pair. If a match is found, the previously selected IP address will be returned.

To ensure the selected IP is still valid for the request, the GSLB controller checks for the following conditions to be true before it returns the reply:

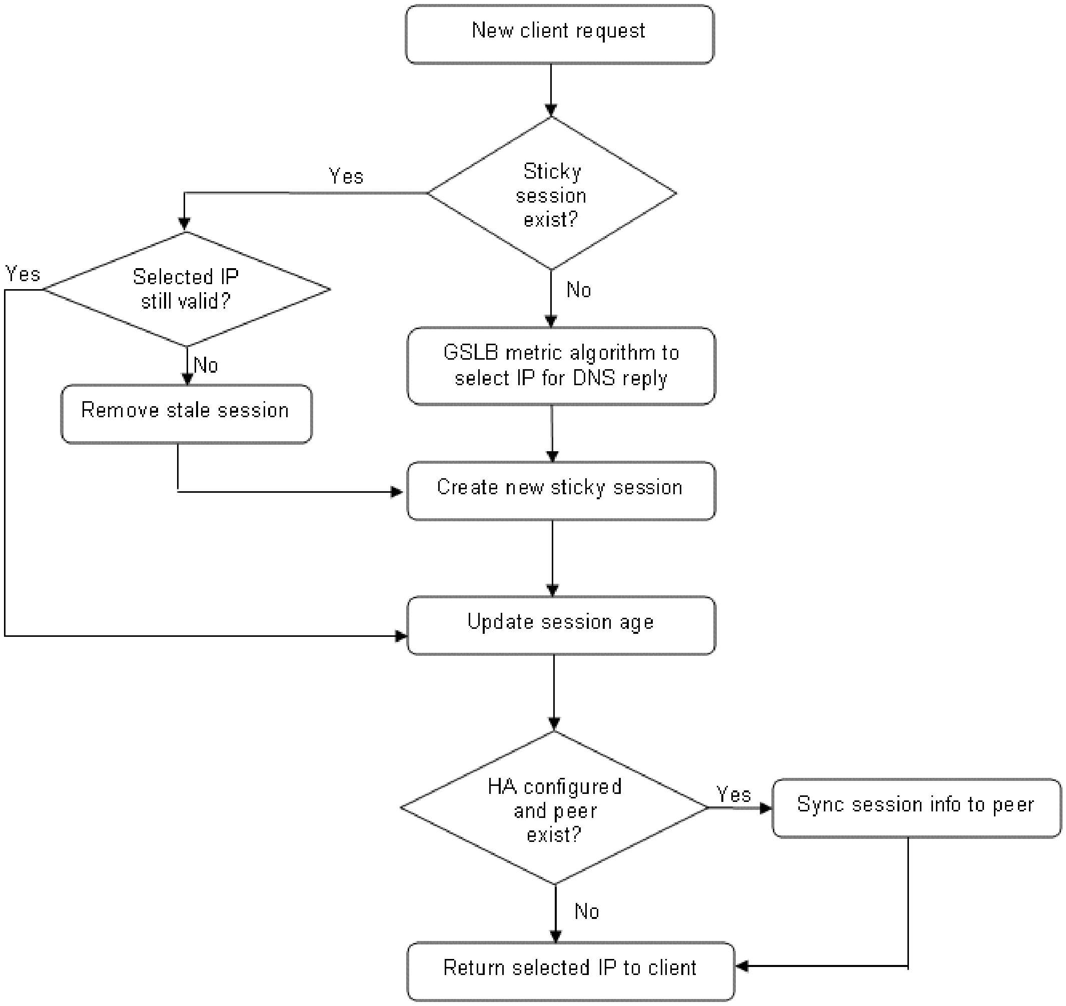
- Selected IP still belongs to the requested domain
- Selected IP is still active

Sticky GSLB is implemented as a GSLB policy, and it can be applied globally or on per host basis.

Algorithm

The following flow diagram illustrates how the Sticky GSLB algorithm works.

FIGURE 4 Flow diagram


New client request
Sticky session exist?
Yes
No
Selected IP still valid?
Yes
No
Remove stale session
GSLB metric algorithm to select IP for DNS reply
Create new sticky session
Update session age
HA configured and peer exist?
Yes
Sync session info to peer
No
Return selected IP to client

Enabling sticky GSLB

Enabling sticky GSLB is the minimum required configuration.

On the GSLB controller, to enable Sticky GSLB globally for all the domains, enter commands such as the following:

```
SLB-Ctrl-ServerIronADX(config)#gslb policy
SLB-Ctrl-ServerIronADX(config-gslb-policy)#sticky
```

On the GSLB controller, to enable Sticky GSLB for a specific host, enter commands such as the following:

```
SLB-Ctrl-ServerIronADX(config)#gslb-host-policy test
SLB-Ctrl-ServerIronADX(config-gslb-host-policy-test)#sticky
SLB-Ctrl-ServerIronADX(config)#gslb dns zone gslb.com
SLB-Ctrl-ServerIronADX(config-gslb-dns-gslb.com)#host-info www gslb-policy test
```

This example defines a host policy, then applies that policy to the specific host www. The **sticky** is one function within the host policy.

Syntax: [no] sticky

NOTE
No special CLI commands need to be issued on the site ServerIron ADX.

Allowing sticky sessions for a specific prefix length

You can allow sticky sessions for a specific prefix length (not all hosts). For added granularity of the sessions, specify the prefix length for the client IPs. The default is 32 bits.

To allow sticky sessions for a specific prefix length, enter commands such as the following:

```
SLB-Ctrl-ServerIronADX(config)#gslb-host-policy test
SLB-Ctrl-ServerIronADX(config-gslb-host-policy-test)#sticky 24
```

Syntax: [no] sticky { <*prefix-length*> | **ipv6-prefix-length** <*prefix-length*> }

The variable<*prefix-length*> specifies the IPv4 prefix length. The default is 32 bits.

The **ipv6-prefix-length** parameter specifies that an IPv6 prefix length. The default is 128 bits.

NOTE
ServerIron ADX does not support the synchronization of sticky sessions across BPs. With sticky prefix-length configured, DNS requests from clients on the same subnet go to different BPs and different sticky sessions will be created on different BPs. However, each individual client will receive the same specific domain-IP that it received in its previous DNS request.

Configuring the sticky GSLB session life time

The Sticky GSLB session life time (age) prevents sessions from hanging for extended periods of time. Sometimes clients do not accept DNS servers, thus creating stale sessions. Use the **sticky age** command to make session resources available to other clients. By default, idle sessions are timed out after five minutes.

To configure the Sticky GSLB session life time (age), enter commands such as the following:

```
SLB-Ctrl-ServerIronADX(config)#gslb-host-policy test
SLB-Ctrl-ServerIronADX(config-gslb-host-policy-test)#stick age 5
```

Syntax: [no] sticky age <*value*>

The <*value*> is the number of minutes before sticky session is cleared.

Displaying current sticky GSLB sessions

To display current Sticky GSLB sessions, rconsole into a barrel processor (BP) and enter the following command.

```
2/3 #show session all 0
Session Info:

Flags - 0:UDP, 1:TCP, 2:IP, 3:INT, 4:INVD, H: sessInHash, N: sessInNextEntry

Index Src-IP         Dst-IP         S-port D-port Age  Next Serv   Flags
===== ======         ======         ====== ====== ===  ==== ==== =========
0      0.0.0.5        100.1.1.10     5      80     0  000000 n/a    SLB1 H
1      0.0.0.5        100.1.1.30     5      80     0  000000 n/a    SLB1 H
2      100.1.1.0      255.0.255.0    7      8      57 000000 n/a    SLB3 H
3      100.1.1.6      0.0.0.1        1      1      60 000000 n/a    SLB1 H
4      100.1.1.7      0.0.0.1        1      1      60 000000 n/a    SLB1 H
5      0.0.0.5        100.1.1.10     5      21     0  000000 n/a    SLB1 H
6      0.0.0.5        100.1.1.30     5      21     0  000000 n/a    SLB1 H
7      0.0.0.5        100.1.1.11     5      53     0  000000 n/a    SLB1 H
8      0.0.0.5        100.1.1.40     5      53     0  000000 n/a    SLB1 H
```

In the example, the default sticky "Age" is five minutes (62-57 = 5). All Sticky GSLB sessions are identified by the following three static numbers that do not change: 255.0.255.0 (Dst-IP), 7 (S-port), and 8 (D-port). Obviously, the client IP (Src-IP) will always change.

Syntax: **show session all** [<*offset*>]

The <*offset*> is the start session number to print.

To show detailed information about the Sticky GSLB session, enter the **detail 2** option.

```
2/3 #show session detail 2
Session at index: 2
sticky GSLB session for client 100.1.1.0
query name www.gslb.com: selected IP 100.1.1.10 by 100.1.1.11
Syntax: show session detail [index]
 Index: the index of sticky GSLB session
```

The client from 100.1.1.0 queries the hostname *www.gslb.com*, and the ServerIron ADX returns the address 100.1.1.10. The VIP that returned the answer is at 100.1.1.11.

Sticky GSLB counters

To display how many times an IP address was selected as the best candidate for a client request, enter the following command.

```
2/3 #show gslb dns detail

ZONE: gslb.com
HOST: www:
(GSLB policy: test)
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*      100.1.1.30: dns v-ip    ACTIVE N-AM      0    0    13 (100%)
                  Active Bindings: 1
                  site: local, weight:   0, SI: 100.1.1.1
                  session util:   0%, avail. sessions: 5999973
                  preference: 128
                  Metric counter (count [selection-metric]):
                  1[least-response]
                  Sticky selection count = 12

*      100.1.1.40: dns v-ip    DOWN   N-AM     --   --    0 (0%)
                  site: local, weight:   0, SI: 100.1.1.1
                  session util:   0%, avail. sessions: 5999973
                  preference: 128
                  preference: 128
                  Not selected yet

*      100.1.1.10: dns v-ip    ACTIVE N-AM      0    0    0 (0%)
                  Active Bindings: 1
                  site: local, weight:   0, SI: 100.1.1.1
                  session util:   0%, avail. sessions: 5999973
                  preference: 128
                  Metric counter (count [selection-metric]):
                  Not selected yet


HOST: ftp:
(Global GSLB policy)
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*      100.1.1.10: dns v-ip    ACTIVE N-AM      0    0    ---
                  Active Bindings: 1
                  site: local, weight:   0, SI: 100.1.1.1
                  session util:   0%, avail. sessions: 5999973
                  preference: 128
```

Notice the line "Sticky selection count = 12". It means 100.1.1.30 was selected 12 times as the best host for a client request. The other IPs have not been selected yet.

Syntax: **show gslb dns detail**

Deleting sticky GSLB session for a specific client

To delete Sticky GSLB sessions for a specific client, enter a command such as the following:

```
ServerIronADX#clear gslb sticky-session client-ip 100.1.1.101
```

Syntax: **clear gslb sticky-session client-ip** <*client-ip*>

The <*client-ip*> is the IP address or prefix of the client for which sticky session will be deleted.

Deleting all sticky GSLB sessions

To delete all the Sticky GSLB sessions globally, enter a command such as the following:

```
ServerIronADX# clear gslb sticky-session all
```

Syntax: **clear gslb sticky-session all**

For a GSLB sticky session to be synced, you must configure symmetric-port with port and VLAN information on both the master and backup ServerIron ADX switches as shown in the following:

```
ServerIronADX(config)# server symmetric-port ethernet 7 vlan-id 7
```

Site persistence in GSLB using hashing

Hash-based GSLB persistence provides GSLB controller persistence in a multiple GSLB controller environment for the same domain. When users query for a host name, regardless of which GSLB controller is contacted, the users will get the same answer.

Sticky GSLB alone is sufficient for single-box and HA (hot standby, symmetric, sym-active) topologies. However, if there are two GSLB controllers across a network providing GSLB for the same domain but are not in an HA configuration, and if persistence is desired when the same client is directed to either of these two GSLB controllers, then hash-based GSLB persistence should be used.

Enabling hash-based GSLB persistence

Hash-based GSLB persistence can be enabled for all domains or only for specific domains. This feature cannot be enabled concurrently with Sticky GSLB in the same policy. Although, you can enable Sticky GSLB for one policy and hash-based GSLB persistence for another policy.

To enable hash-based GSLB persistence globally, enter commands on the GSLB controller, such as the following:

```
SLB-ServerIronADX(config)# gslb policy
SLB-ServerIronADX(config-gslb-policy)# hash-persist
```

Syntax: **hash-persist**

Displaying the hash table

A hash table is maintained for a domain for which hash-based GSLB persistence is enabled in the associated policy. There are 256 entries in the hash table, and there is a domain IP address associated with each of these entries.

To display the hash table for all domains or a specific zone-name, enter a command on the BP, such as the following:

```
ServerIronADX# rconsole 1 1
ServerIronADX1/1#show gslb phash table all
```

Syntax: **show gslb phash table**

This command displays different results depending on which CPU you're looking at. To view a full count of all buckets, you need to examine the hashing table on all BP CPUs, not just one.

When you use "show gslb phash table" on WSM CPUs to view bucket hit counts, the counter that gets incremented depends on which CPU you look at. This happens because client IPs are handled by BP CPUs in a "round robin" methodology.

The bucket hit counts for a given client IP are recorded only on the BP CPU that handled that client's DNS queries.

Example

Start with a client IP of 10.15.102.10 and send five queries.
Change the client IP to 10.15.102.11 and send four queries.
Change the client IP to 10.15.102.12 and send three queries.
Change the client IP to 10.15.102.13 and send two queries.
Change the client IP to 10.15.102.14 and send one query.

If you rconsole to each CPU and check "show gslb phash table all", the bucket hit counter that gets incremented changes depending on which CPU you view.

```
rconsole 1 1:
backet 137: ip 10.15.101.162, hit count 0
backet 138: ip 10.15.101.161, hit count 0
backet 139: ip 10.15.101.162, hit count 3
backet 140: ip 10.15.101.161, hit count 0
backet 141: ip 10.15.101.162, hit count 0

rconsole 1 2:
backet 137: ip 10.15.101.162, hit count 5
backet 138: ip 10.15.101.161, hit count 0
backet 139: ip 10.15.101.162, hit count 0
backet 140: ip 10.15.101.161, hit count 2
backet 141: ip 10.15.101.162, hit count 0

rconsole 1 3:
backet 137: ip 10.15.101.162, hit count 0
backet 138: ip 10.15.101.161, hit count 4
backet 139: ip 10.15.101.162, hit count 0
backet 140: ip 10.15.101.161, hit count 0
backet 141: ip 10.15.101.162, hit count 1

The BP responsible changes depending on the bucket.
```

Hashing scheme

The client IP address is hashed to generate a value between 0 and 255 as follows.

The 32-bit client IP address is split into four 8-bit quantities and bit-wise addition is performed to yield a hash index between 0 and 255. The hash index is an 8-bit quantity.

Example

1.1.1.42 yields hash index 45 {(1+1+1+42 %256) = 45}

172.168.10.1 yields hash index 95 {(172+168+10+1 %256) = 95}

After the Client IP address is hashed to an index in the hash table, the IP address associated with the hash index in the hash table is selected as the best IP address for the client. The ServerIron reorders the IP address in the DNS server's response so that the best IP address is first. Then it forwards the modified response to the client.

IP address allocation

IP addresses are first ordered with the lowest IP having rank 1. IPs are allocated to hash buckets in a round robin fashion starting with lowest IP first.

Example

Assume a user has configured IPs 1.1.1.44 and 1.1.1.42 for *www.foo.com*. The IP addresses are sorted in ascending order.

1.1.1.42 (rank 1)
1.1.1.44 (rank 2)

The hash allocation for *www.foo.com* looks like the following:

0	1	2		255
.42	.44	.42	....	.44

If the IP address of a client querying for *www.foo.com* hashes to hash index 2, then 1.1.1.42 will be selected as the best IP address for this client.

IP address failure or removal from domain

In the previous example, assume a user removes 1.1.1.44 for domain *www.foo.com*. The IP address for *www.foo.com* is 1.1.1.42 (rank 1)

In this scenario, all the hash indexes allocated to 1.1.1.44 will be cleaned up. All the empty hash indexes will be reassigned to existing IP addresses in round robin fashion as described in the section "IP Address Allocation".

0	1	2		255
.42	.42	.42	....	.42

Rehash: new IP address for a domain or change of state

This section describes how the ServerIron ADX handles the introduction of a new IP address for a domain or change of state of an IP address from down to healthy (rehash mechanism).

Assume the hash-table size is 10, and the following IP addresses are configured for *www.foo.com*.

1.1.1.42 (rank 1)
1.1.1.44 (rank 2)

The hash table allocation looks like the following:

0	1	2	3	4	5	6	7	8	9
.42	.44	.42	.44	.42	.44	.42	.44	.42	.44

Now the new IP address 1.1.1.43 is configured for domain *www.foo.com*.

The ServerIron ADX sorts the IP addresses for domain *www.foo.com* as follows.

1.1.1.42 (rank 1)
1.1.1.43 (rank 2)
1.1.1.44 (rank 3)

The new IP is 1.1.1.43.

The top row below shows the current allocation of the hash table. With the new set of IPs, the ServerIron ADX needs to get this hash table in the state shown in the bottom row.

0	1	2	3	4	5	6	7	8	9
.42	.44	.42	.44	.42	.44	.42	.44	.42	.44
.42	.43	.44	.42	.43	.44	.42	.43	.44	.42

```
{For hash index h, the IP allocated to it will be the IP whose rank is equal to:
    (h % num-ips) + 1

    In the above example, num-ips = 3
    Hash index 0: allocate IP with rank 0%3 + 1 i.e. rank 1 i.e. 1.1.1.42
    Hash index 1: allocate IP with rank 1%3 + 1 i.e. rank 2 i.e. 1.1.1.43
    Hash index 2: allocate IP with rank 2%3 + 1 i.e. rank 3 i.e. 1.1.1.44
    Hash index 4: allocate IP with rank 3%3 + 1 i.e. rank 1 i.e. 1.1.1.42
    ...and so on
}
```

Change the allocations in row 1 to match row 2.

0	1	2	3	4	5	6	7	8	9
.42	.43	.44	.42	.43	.44	.42	.43	.44	.42

The hash-table allocation will be the same after the introduction of a new IP, on all the GSLB controllers with the same set of IPs for the domain. At the same time, this method will preserve some of the original assignments and provide fair allocation to the newly introduced IP without the need for a protocol between two or more network redundant GSLB controllers.

If this mechanism is used for two controllers in HA, no hash table synchronization will be required between them.

Disabling rehash

You can disable rehash on the introduction of a new IP address or change of IP address state from down to healthy. It programs the ServerIron ADX to avoid the breaking of persistence that occurs when rehashing is performed. The trade-off is the new IP address will not be included in the hash table.

To disable rehash, enter commands such as the following:

```
SLB-ServerIronADX(config)#gslb policy
SLB-ServerIronADX(config-gslb-policy)#hash-persist persist-rehash-disable
```

The second command disables the behavior described in the section “Rehash: new IP address for a domain or change of state” on page 72.

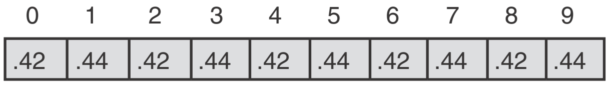
Syntax: **hash-persist persist-rehash-disable** <*time-out*>

The <*time-out*> parameter specifies the number of seconds before an IP address is removed from the hash table when that IP becomes down. The default is 5 seconds.

Consider the example where a user has configured this command and set the following IP addresses for *www.foo.com*.

1.1.1.42 (rank 1)
1.1.1.44 (rank 2)

The hash table allocation is as follows.



0	1	2	3	4	5	6	7	8	9
.42	.44	.42	.44	.42	.44	.42	.44	.42	.44

If the user now configures a new IP address 1.1.1.43 for domain *www.foo.com* and this IP address is healthy, the controller will still not do any reassignments of the hash buckets to this new IP address to preserve persistence for all hash buckets.

Hash-persist hold-down: boot up considerations if rehash disabled

If rehash is disabled, then rehash on introduction of new IP address or change of IP address state from down to healthy is disabled. However, the boot up case must be taken into account.

After the GSLB ServerIron ADX boots up, it will perform a back-end query for the IP addresses associated with the domain. Once it obtains these addresses, the ServerIron ADX will determine their health. The health of some of the IPs may be determined by health checks done by the GSLB ServerIron ADX and some by means of distributed health check. Therefore after boot up, the IPs may come up one after another instead of at the same time. If rehash is disabled, a rehash must still be performed for this case.

To specify how long the disabling of rehash becomes effective after boot up, enter a command such as the following:

```
SLB-ServerIronADX(config)#gslb policy
SLB-ServerIronADX(config-gslb-policy)#hash-persist hold-down 5
```

Syntax: **hash-persist hold-down** <*time*>

The <*time*> parameter specifies the number of minutes (1-255) before rehash disable become effective after boot up. The default is five minutes.

Manually forcing rehash for a domain

Consider the case where you disable rehashing on introduction of a new IP address or change of IP address state from down to healthy, such as described in the previous section.

In such a scenario, you may wish to force a rehash at a feasible time in order to allow the new IP addresses to also be included in the hash table. For this case, to manually rehash the hash table, enter a command such as the following:

```
SLB-ServerIronADX#clear gslb phash table zone-name gslb.com host-name www
```

Syntax: **clear gslb phash zone-name** <*zone-name*> **host-name** <*host-name*>

Show commands

Many existing **show** commands for GSLB global and host-level policy have been enhanced for hash-based persistence. Take note of the **bold** fields.

```
SLB-ServerIronADX#show gslb policy

  Default metric order: ENABLE
  Metric processing order:
                1-Server health check
                2-Remote SI's session capacity threshold
                3-Round trip time between remote SI and client
                4-Geographic location
                5-Remote SI's available session capacity
                6-Round-robin selection


  DNS active-only: DISABLE  DNS best-only: DISABLE  DNS override: DISABLE
  DNS cache-proxy: DISABLE  DNS transparent-intercept: DISABLE
  DNS cname-detect: DISABLE  Modify DNS response TTL: ENABLE
  DNS TTL: 10 (sec), DNS check interval: 30 (sec)
  Remote SI status update period: 30 (sec)
  Remote SI health-status update period: 5 (sec)
  Session capacity threshold: 90%  Session availability tolerance: 10%
  Round trip time tolerance: 10%, round trip time explore percentage:5%
  Round trip time cache prefix: 20, round trip time cache interval: 120 (sec)
  Round trip time cache age refresh: DISABLE
  Round trip time algorithm selection:  USE PASSIVE ONLY
  Connection load: DISABLE
  Weighted Site Metric: DISABLE     Weighted IP Metric: DISABLE
  Active Bindings Metric: DISABLE
  persistent hashing: ENABLE
  persistent hashing rehash disabled: ENABLE
```

```
SLB-ServerIronADX#show gslb dns detail

ZONE: gslb.com
HOST: www:
(Global GSLB policy)
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*     100.1.1.163: dns v-ip    ACTIVE N-AM      0    0    7 (100%)
                  Active Bindings: 1
                  site: local, weight:   0, SI: 100.1.1.2
                  session util:   0%, avail. sessions: 5999865
                  preference: 128
                  Metric counter (count [selection-metric]):
                  Not selected yet
                  persistent hash selection count = 7
```

In the previous screen shot, the field "persistent hash selection count =7" means IP 100.1.1.163 had been selected 7 times in result of a match in the hash persistent policy.

To display the hash table for a domain for which hash-based persistence is enabled, enter the following command on the BP.

```
SLB-ServerIronADX2/2# show gslb phash table zone-name gslb.com host-name www
```

It displays the hash index, associated domain IP, and hit count for each hash entry.

Syntax: **show gslb phash table zone-name** <*name*> **host-name** <*name*>

Weighted distribution of sites with hash-based persistence

This section contains the following subsections:

- "Overview of distribution of sites with hash-based persistence" on page 76
- "Configuring distribution of sites with hash-based persistence" on page 79

Overview of distribution of sites with hash-based persistence

This section contains the following sub-sections:

- "GSLB hash-based persistence" on page 77
- "GSLB weighted hash-based persistence" on page 77
- "Hashing scheme" on page 77
- "IP address allocation" on page 77
- "IP address failure or removal from domain" on page 78
- "Rehashing for new IP address for a domain or state change from down to up" on page 78
- "Rehash: change in hash weight" on page 79
- "Disabling rehash on introduction of new IP addresses or state change from down to healthy" on page 79

- "Disabling rehash on change in hash weight configuration" on page 79

GSLB hash-based persistence

GSLB provides two methods for persistence- Sticky method and Hash-based persistence. Sticky GSLB is suitable for single-box and HA (hot standby, symmetric, sym-active) topologies. However, if there are two GSLB controllers across a network providing GSLB for the same domain but are not in an HA configuration, and if persistence is desired when the same client is directed to either of these two GSLB controllers, then hash-based GSLB persistence should be used. hash-based Persistence provides GSLB controller persistence in multiple GSLB controller environments. When users perform a DNS query for a domain, the users will get the same IP address for that domain regardless of which GSLB controller is contacted. Currently hash-based persistence distributes hash buckets in a round robin fashion.

GSLB weighted hash-based persistence

In addition to providing hash-based persistence, we will now provide weighted hash-based persistence. Weighted hash-based persistence allocates the hash buckets in a weighted round robin fashion. This enables the user not only to maintain persistence, but also to determine what percentage of the traffic goes to a particular domain IP address.

Hashing scheme

Each domain maintains a separate hash table. For instance, if GSLB controller has the following two domains *www.foo.com* and *www.test.com* configured, then it will maintain one hash table for each domain. The number of hash buckets for each hash table is 256.

The client IP address is hashed to generate a value between 0 and 255.

After the Client IP address is hashed to an index in the hash table, the IP address associated with the hash index in the hash table is selected as the best IP address for the client. The GSLB controller reorders the IP address in the DNS server's response so that the best IP address is placed in the first position. It then forwards the modified response to the client.

IP address allocation

Firstly, IP addresses are ordered with the lowest IP having rank 1. IPs will be allocated to hash buckets in a weighted round robin fashion starting with lowest IP first. This is done so that no synchronization is required across Controllers.

Example

Consider the example where user has configured IPs 1.1.1.44, 1.1.1.43 and 1.1.1.42 for *www.foo.com*. The IP addresses are first sorted in ascending order.

```
1.1.1.42 (rank 1)
1.1.1.43 (rank 2)
1.1.1.44 (rank 3)
```

User also configures hash weights for these IP addresses. Say the weights for the IP addresses are as follows.

```
1.1.1.42: weight 1
1.1.1.43: weight 1
1.1.1.44: weight 2
```

In our example,

```
Hash bucket 0 will be assigned to 1.1.1.42
Hash bucket 1 will be assigned to 1.1.1.43
Hash bucket 2 will be assigned to 1.1.1.44
Hash bucket 3 will be assigned to 1.1.1.44
Hash bucket 4 will be assigned to 1.1.1.42
Hash bucket 5 will be assigned to 1.1.1.43
Hash bucket 6 will be assigned to 1.1.1.44
Hash bucket 7 will be assigned to 1.1.1.44
```

And so on.

In other words, for every bucket assigned to 1.1.1.42, one will be assigned to 1.1.1.43 and two will be assigned to 1.1.1.44 i.e. assignments will be done in a round robin manner in proportion to the hash weights.

The hash table for *www.foo.com* will be as follows.

0	1	2	3		255
.42	.43	.44	.44		.44

If the IP address of a client querying for *www.foo.com* hashes to hash index 2, then 1.1.1.44 will be selected as the best IP address for this client.

IP address failure or removal from domain

In the previous example, assume user removes 1.1.1.44 for domain *www.foo.com*. The IP addresses remaining for *www.foo.com* are as follows.

```
1.1.1.42 (rank 1)Hash weight 1
1.1.1.43 (rank 2)Hash weight 1
```

In this scenario, all the hash indexes allocated to 1.1.1.44 will be reassigned to 1.1.1.42 and 1.1.1.43 in proportion to their weights.

The basic algorithm used will be same as that described in section 1.3. The difference is that only buckets that have been assigned to 1.1.1.44 will be reassigned.

Rehashing for new IP address for a domain or state change from down to up

This section describes how the ServerIron ADX handles the introduction of a new IP address for a domain or change of state of an IP address from down to healthy.

For example, following IP addresses are configured for *www.foo.com*.

```
1.1.1.42 (rank 1)Hash Weight: 1
1.1.1.43 (rank 2) Hash Weight: 1
```

The hash table allocation looks like the following:

0	1	2	3		255
.42	.43	.42	.43		.43

Now the new IP address 1.1.1.44 is configured for domain *www.foo.com*.

The ServerIron ADX sorts the IP addresses for domain *www.foo.com* in ascending order of the addresses as follows.

```
1.1.1.42 (rank 1)Hash Weight: 1
1.1.1.43 (rank 2)Hash Weight: 1
1.1.1.44 (rank 3) Hash Weight: 2
```

The hash table for domain is rehashed using the algorithm described in Section 1.3. The hash table for *www.foo.com* will be as follows after rehashing.

0	1	2	3		255
.42	.43	.44	.44		.44

The hash-table allocation will be the same after the introduction of a new IP, on all the GSLB controllers with the same set of IPs for the domain. At the same time, this method will provide fair allocation to the newly introduced IP without the need for a protocol between two or more network redundant GSLB controllers. Even if this mechanism is used for two controllers in HA, no hash table synchronization is required between them.

Disabling rehash on introduction of new IP addresses or state change from down to healthy

You can disable rehash on the introduction of a new IP address or change of IP address state from down to healthy. User would typically disable this rehash to avoid breaking the persistence when rehashing is performed. The trade off is the new iP address will not be included in the hash table. User will have to manually rehash at a later time to enable the new IP address to be included.

If the rehashing on state change or introduction of a new IP is disabled, and such an event occurs, then a message stating that the ServerIron ADX needs to be rehashed at a later time will be displayed.

Rehash: change in hash weight

ServerIron ADX will rehash the hash table for a domain when the hash weight for an IP configured for the domain is changed. The rehashing will be similar to that described in Section 1.4.

Disabling rehash on change in hash weight configuration

You can disable rehash on change in hash weight configuration for domain IP addresses. User would typically disable this rehash to avoid breaking the persistence when rehashing is performed due to change in hash weight. The trade-off is the new weight for the IP address will not be reflected in the hash bucket assignments for the hash table. User will have to manually rehash at a later convenient time to enable the new weight to be used in hash table assignments.

Configuring distribution of sites with hash-based persistence

With the weighted hash-based GSLB persistence, users will be able to define hash weights for IPs for a domain. The hash buckets will be distributed among the domain IP addresses in proportion to these weights.

The new command line interface needed for weighted hash-based GSLB persistence is described below.

NOTE
All the existing CLI for old hash-based persistence is applicable to weighted hash based persistence also. It is not described in this document for the sake of brevity. For further details on existing CLI for hash-based persistence, please refer to the online GSLB documentation.

Enabling weighted hash-based GSLB persistence

Weighted hash-based GSLB persistence can be enabled for all domains or for specific domains as needed. User enables this feature in the global or host-level policy. As a result, this feature applies to all the domains this policy is bound to. This feature cannot be enabled concurrently with Sticky GSLB in the same policy. However you can enable Sticky GSLB for one policy and Weighted hash-based GSLB persistence for another policy.

To enable Weighted hash-based GSLB persistence globally, enter commands on the GSLB controller, such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# hash-persist  weighted
```

To enable Weighted hash-based GSLB persistence for a host-level policy, enter commands on the GSLB controller, such as the following:

```
ServerIronADX# config t
ServerIronADX(config)# gslb-host-policy test
ServerIronADX(config-gslb-host-policy-test)# hash-persist  weighted
```

Syntax: [no] hash-persist [weighted]

NOTE
Note that "**weighted**" is an optional parameter. If "weighted" is not specified, then the old hash-based persistence mechanism will be in effect. The old hash-based persistence mechanism distributes the hash buckets in a round robin manner. If the mechanism is changed from hash-based persistence to weighted hash-based persistence or vice versa in a GSLB global or host-level policy, then the hash table for all domains associated with that policy will be rehashed.

GSLB hash based site persistence with configurable subnet mask length

ServerIron ADX allows specification of subnet mask while doing GSLB site persistence. The LB controller hashes the entire 32-bits of a LDNS IP address to generate the hash bucket for GSLB hash-based persistence. As a result, LDNS servers in the same subnet could be assigned to different hash buckets. We now provide a mechanism for the user to define a subnet length for hashing; only this portion of the LDNS IP address will be used to generate the hash bucket. As a result, user can ensure that all the LDNS servers that fall in the same subnet, as defined by the hash prefix length, will hash to the same bucket and be serviced by the same domain IP address. As an example, if the specified source subnet mask is /24 then all LDNS servers within a given /24 subnet would receive same response (site IP) from the GSLB controller.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# prefix-len-hash-persist  24
```

Syntax: [no] prefix-len-hash-persist *<length>*

NOTE
This command should be configured under the gslb global or host-level policy.

Configuring weights for domain IP addresses

Weighted Hash-based GSLB persistence enables the user to distribute the hash buckets for the domain in proportion to the weights configured for the domain IP addresses. Use the following command line interface to configure weights for the domain IP addresses.

```
ServerIronADX(config)# gslb dns zone gslb.com
ServerIronADX(config-gslb-dns-gslb.com)# host www http
ServerIronADX(config-gslb-dns-gslb.com)# host www ip-hash-weight 20.20.1.80 10
ServerIronADX(config-gslb-dns-gslb.com)# host www ip-hash-weight 30.30.1.80 20
```

Syntax: **host-info** <*host-name*> **ip-hash-weight** <*IPaddress*> <*weight*>

- The <*host-name*> parameter specifies the host name.
- <*IP address*> is the IP address for which you are assigning a hash weight.
- <*weight*> is a value from 0 to 100. The default value is 1. A weight of 0 implies that the client IP will not be allocated any hash buckets. A weight of 0 can be used to designate a domain IP as backup.

NOTE
The aggregate of the hash weights for all the IPs for a domain does not have to add up to 100.

When user configures a hash weight of zero for a domain IP, no hash buckets are allocated to this domain IP. If the hash buckets for this domain does not have any other healthy IPs, then the best IP address among all the healthy IPs including the IP with hash weight of zero, will be selected based on the remaining GSLB metrics. So user can configure a domain IP to be used as a backup IP by configuring a weight of zero for this IP address.

Disabling rehash on introduction of new IP addresses or state change from down to healthy

You can disable rehash on the introduction of a new IP address or change of IP address state from down to healthy. Persistence that occurs when rehashing is performed is prevented. The trade-off is the new IP address will not be included in the hash table.

To disable rehash, enter commands such as the following:

```
SLB-ServerIronADX(config)# gslb policy
SLB-ServerIronADX(config-gslb-policy)# hash-persist persist-rehash-disable
```

Syntax: **hash-persist persist-rehash-disable** <*time-out*>

The <*time-out*> parameter specifies the number of seconds before an IP address is removed from the hash table when that IP becomes down. The default is 5 seconds.

Disable rehash when weight for an IP is changed

When user changes the hash weight configured for an IP in the domain, GSLB controller will automatically rehash the hash table for that domain. You can disable this rehash on weight configuration change with the following command.

Use the following command line interface to disable rehashing on weight change for global GSLB policy.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# hash-persist disable-weight-rehash
```

Use the following command line interface to disable rehashing on weight change for host-level GSLB policy.

```
ServerIronADX# config t
ServerIronADX(config)# gslb-host-policy test
ServerIronADX(config-gslb-host-policy-test)# hash-persist disable-weight-rehash
```

Syntax: [no] hash-persist disable-weight-rehash

If the weight of an IP for a domain is changed and this command is configured, then a message, stating that the ServerIron ADX needs to be rehashed at a later time, will be displayed.

If user configures this command, he or she will have to manually rehash at a later convenient time. This command can be used when user does not want to break the persistence for the existing IP addresses due to a change in weight configuration. User will disable rehashing on weight configuration change to preserve persistence and instead will rehash manually at a later convenient time, such as during a maintenance window for the GSLB controller.

Hash persist hold down timer

Hash persist hold down timer is provided to handle the boot up case when rehash on state change from down to up or rehash on weight configuration change is disabled. This hold down timer specifies how long after boot up, the disabling of rehash on state or weight change takes effect. Any change to the configured hash weight will result in a rehash during the hold-down time i.e. even if you have disabled rehash on weight change, it will become effective only after this hold-down time has elapsed.

After the GSLB ServerIron ADX boots up, it will perform a back-end query for the IP addresses associated with the domain. Once it obtains these addresses, the ServerIron ADX will determine their health. Therefore after boot up, the IPs may come up one after another instead of at the same time. The weights will get associated with the IPs as they come up; this means that even if rehash is disabled, a rehash must still be performed to handle this scenario.

To specify how long the disabling of rehash on weight change becomes effective after boot up, enter a command such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# hash-persist hold-down 5
```

Syntax: hash-persist hold-down <*time*>

Syntax: [no] hash-persist hold-down <*time*>

- The <*time*> parameter specifies the number of minutes (1-255) before rehash disable become effective after boot up.
- The default is five minutes.

NOTE
This command is provided in the existing hash-based persistence. The same command will be used for the weighted hash-based persistence as well.

Manually forcing rehash for a domain

Consider the case where user disables rehashing on introduction of a new IP address or change of IP address state from down to healthy or on change in the IP weight configuration, as described earlier.

In such a scenario, user may wish to force a rehash at a feasible time in order to allow the new configuration to also be included in the hash table. User can manually rehash the hash table by using the following command.

```
ServerIronADX# clear gslb phash table zone-name gslb.com host-name www
```

Syntax: **clear gslb phash table [zone-name** <*zone-name*> **host-name** <*host-name*> **| all]**

Clear GSLB phash counters

```
ServerIronADX# clear gslb phash counter
```

Syntax: **clear gslb phash counter [all | zone-name** <*name*> **host-name** <*name*>**]**

Show commands

NOTE
The following commands should be used on the Barrel Processors only. You should use the "rconsole <*slot*> <*processor*>" command to go to the desired Barrel Processor and then use these commands on the Barrel Processor.

The following command will display whether weighted hash-based persistence is enabled for global GSLB policy or not.

Syntax: **show gslb policy**

The following command will display whether weighted hash-based persistence is enabled for host-level GSLB policy or not.

Syntax: **show gslb policy host-policy-name** <*policy-name*>

The following command will display the hash table and related information for all domains or for a specific domain.

Syntax: **show gslb phash table [all | zone-name** <*name*> **host-name** <*name*>**]**

The following command will display hash bucket number of a client IP address and DNS domain IP that is associated with that hash bucket. This command will also display the number of hashed and active DNS domain IPs for the given domain.

Syntax: **show gslb phash allocation** <*client-ip-address*> <*zone-name*> <*host-name*>

The command should be used on Barrel Processors only. User should use the "rconsole <*slot*> <*processor*>" command to go the desired Barrel Processor and should use this command on the Barrel Processor.

Here is the sample output of this command.

```
=========================================================================
==========

GSLB-Controller-A1/1# show gslb phash allocation 30.30.1.2 l47qa.com www
********************************************************
        GSLB weighted persist hash
```

```
********************************************************
Client IP address: 30.30.1.2
Domain : www.l47qa.com
Number of hashed IPs for domain : 3
Number of active IPs for domain : 3
Client IP hashes to bucket number: 63
IP associated with hash bucket 63: 20.20.1.100
Your Client IP 30.30.1.2 will be serviced by domain IP 20.20.1.100
```

Displaying weighted hash-based GSLB persistence

The following command will show the list of active DNS domain IPs of a zone, weight value configured for each IP, number of hash buckets allocated for each IP and usage counter for each IP.

Syntax: **show gslb phash active-ip** [**all** | **zone-name** <*name*> **host-name** <*name*>]

The command should be used on Barrel Processors only. User should use the "rconsole <*slot*> <*processor*>" command to go the desired Barrel Processor and should use this command on the Barrel Processor.

Here is the sample output of this command.

```
ServerIronADX# show gslb phash active-ip all
Persistent Hash active IP address for www.l47qa.com
active IP: 20.20.1.100, weight: 100, buckets: 212, usage: 0
active IP: 30.30.1.100, weight: 10, buckets: 22, usage: 0
active IP: 40.40.1.100, weight: 10, buckets: 22, usage: 0
```

Debug command

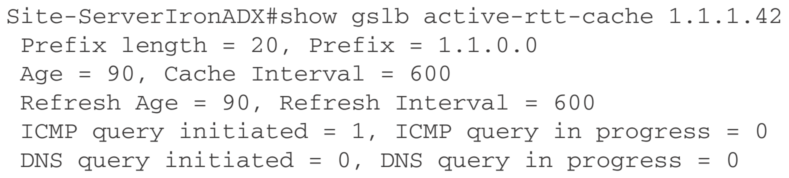
User can configure the following command to enable debugging for weighted hash-based GSLB persistence.

```
ServerIronADX# debug phash
```

Syntax: [**no**] **debug phash**

Displaying the contents of active RTT cache entries

To display the contents of the active RTT cache entries on the site ServerIron ADX, enter a command such as the following:



```
Site-ServerIronADX#show gslb active-rtt-cache 1.1.1.42
 Prefix length = 20, Prefix = 1.1.0.0
 Age = 90, Cache Interval = 600
 Refresh Age = 90, Refresh Interval = 600
 ICMP query initiated = 1, ICMP query in progress = 0
 DNS query initiated = 0, DNS query in progress = 0
```

Syntax: **show gslb active-rtt-cache** <*ldns-ip*>

The <*ldns-ip*> refers to the IP address of the local DNS server for which you want to display the corresponding prefix entry in the site ServerIron ADX active RTT cache.

Affinity

The GSLB affinity feature configures the GSLB ServerIron ADX to always prefer a specific site ServerIron ADX for queries from clients whose addresses are within a given IP prefix. This feature is useful in the following situations:

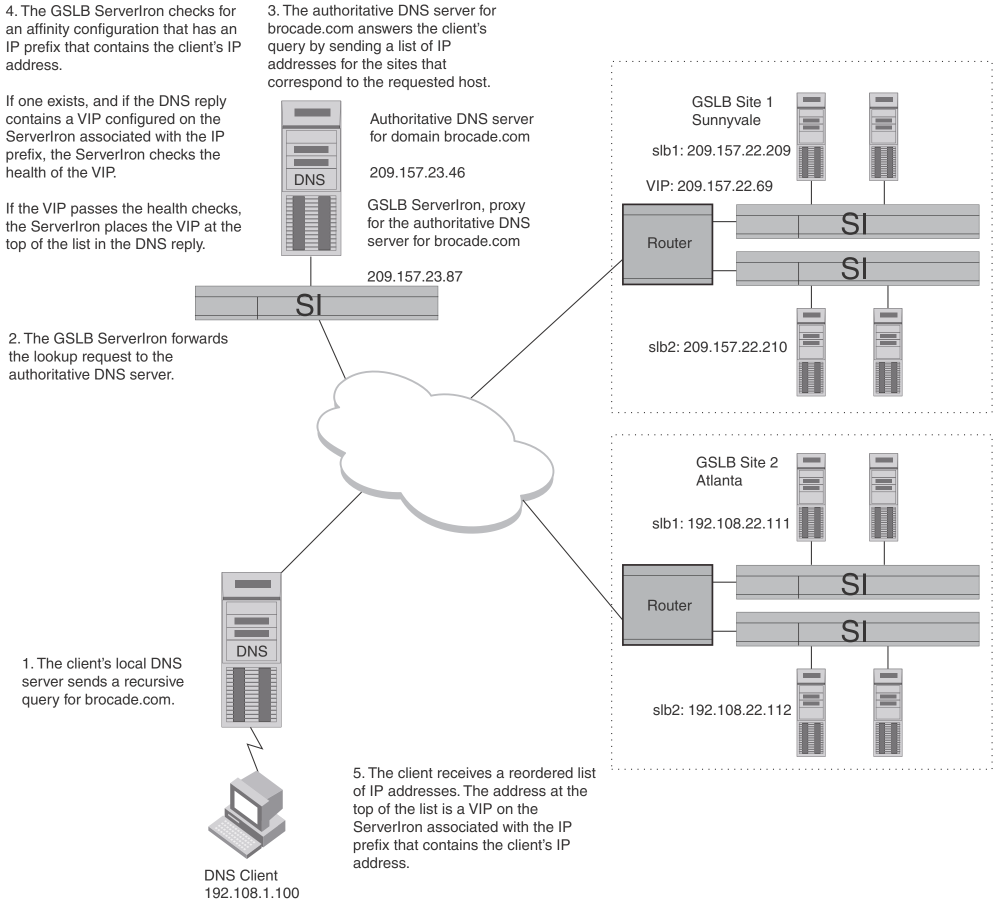
- When you want to use a primary site for all queries and use other sites only as backups.
- When you want to use a site located near clients within a private network for all queries from the private network.

To configure affinity, you associate a site ServerIron ADX with an IP prefix. When the GSLB ServerIron ADX receives a query from a client whose IP address is within the configured prefix, the GSLB ServerIron ADX examines the DNS reply for a virtual IP address (VIP) configured on the ServerIron ADX associated with the IP prefix that contains the client's IP address.

Figure 5 shows an example of the affinity feature. In this example, the GSLB ServerIron ADX contains the following affinity configuration:

- IP prefix: 192.0.0.0/8, site ServerIron ADX: 209.157.22.209 (slb1 in the sunnyvale site)

FIGURE 5 Example of the affinity feature


4. The GSLB ServerIron checks for an affinity configuration that has an IP prefix that contains the client's IP address.

If one exists, and if the DNS reply contains a VIP configured on the ServerIron associated with the IP prefix, the ServerIron checks the health of the VIP.

If the VIP passes the health checks, the ServerIron places the VIP at the top of the list in the DNS reply.

3. The authoritative DNS server for brocade.com answers the client's query by sending a list of IP addresses for the sites that correspond to the requested host.

2. The GSLB ServerIron forwards the lookup request to the authoritative DNS server.

1. The client's local DNS server sends a recursive query for brocade.com.

5. The client receives a reordered list of IP addresses. The address at the top of the list is a VIP on the ServerIron associated with the IP prefix that contains the client's IP address.

In Figure 5, the client's IP address is within the configured affinity prefix, so the ServerIron ADX checks the DNS reply for a VIP configured on the ServerIron ADX associated with the prefix:

- If the reply contains a VIP on the ServerIron ADX associated with the prefix that the client's IP address is in, the ServerIron ADX places the VIP at the top of the address list in the reply. (This assumes that the VIP passes the applicable health checks if they are enabled.)
- If the reply contains more than one VIP on the ServerIron ADX associated with the prefix that contains the client's IP address, the ServerIron ADX selected the VIP that has been selected least often. (This is the last metric in the GSLB policy and is used as a tiebreaker).
- If the VIP fails a health check, or if the reply does not contain a VIP on the ServerIron ADX associated with the prefix that contains the client's IP address, the ServerIron ADX uses the other GSLB metrics in the policy to reorder the list.

You can configure up to 50 affinities. The IP prefix in each affinity can have a value from 0-31. You can associate only one ServerIron ADX with a prefix. However, you can associate multiple prefixes with the same ServerIron ADX.

If you configure more than one affinity, it is possible for a client's IP address to be within the prefixes of more than one affinity definition. In this case, the ServerIron ADX uses the affinity whose prefix is a more specific match for the client. For example, assume that the GSLB ServerIron ADX in Figure 5 contains the following affinities:

- IP prefix: 192.0.0.0/8, site ServerIron ADX: 209.157.22.209 (slb1 in the sunnyvale site)
- IP prefix: 192.108.0.0/16, site ServerIron ADX: 209.157.22.210 (slb2 in the sunnyvale site)

The client IP address 192.108.1.100 falls within both prefixes. However, prefix 192.108.0.0/16 is a more precise match than prefix 192.0.0.0/8. Therefore, the ServerIron ADX uses the affinity definition that contains prefix 192.108.0.0/16. If the VIP for the more precise prefix is not available (for example, if it fails a health check), the ServerIron ADX uses the standard GSLB policy to select the best site.

You can configure a default affinity definition by using the prefix 0.0.0.0/0 in the definition. When you configure a default affinity definition, the ServerIron ADX prefers a VIP on the ServerIron ADX associated with the prefix 0.0.0.0/0 for all clients except those whose addresses are within a prefix configured in another affinity definition. Configuring a default affinity definition is optional. If you do not configure one, the ServerIron ADX uses the standard GSLB policy for clients whose addresses are not within the prefix of an affinity definition.

Defining the affinity

To enter the GSLB affinity configuration level, enter the following command.

```
ServerIronADX(config)#gslb affinity
ServerIronADX(config-gslb-affinity)#
```

Syntax: gslb affinity

Once you are there, refer to the ServerIron ADX by its GSLB site name and ServerIron ADX name or by its management IP address, by entering the following command.

```
ServerIronADX(config-gslb-affinity)#prefer ?
  ASCII string   site name
  A.B.C.D        ServerIronADX management address
```

Syntax: [no] prefer *<site-name> <si-name>* **|** *<si-ip-addr>* **for** *<ip-addr> <ip-mask>* **|** *<ip-addr>***/***<prefix-length>*

The *<site-name>* and *<si-name>* parameters specify the remote site and a ServerIron ADX at that site. If you use this method, you must specify both parameters.

The *<si-ip-addr>* parameter specifies the site ServerIron ADX's management IP address.

NOTE
In either case, the running-config and the startup-config file refer to the ServerIron ADX by its IP address.

The *<ip-addr> <ip-mask>* or *<ip-addr>/<prefix-length>* parameter specifies the prefix. You can specify a mask from 0.0.0.0-255.255.255.254. If you instead specify a prefix length, you can specify from 0-31 bits.

If you specify 0.0.0.0 0.0.0.0 or 0.0.0.0/0, the ServerIron ADX applies the affinity definition to all client addresses. As a result, an address that does not match another affinity definition uses the zero affinity definition by default. If you do not configure a default affinity definition, the ServerIron ADX uses the standard GSLB policy for clients whose addresses are not within a prefix in an affinity definition.

```
ServerIronADX(config-gslb-affinity)# prefer sunnyvale slb-1 for 0.0.0.0/0
ServerIronADX(config-gslb-affinity)# prefer atlanta slb-1 for 192.108.22.0/22
```

These commands configure a default affinity definition (using the 0.0.0.0/0) prefix and an affinity definition that uses prefix 192.108.22.0/22. For clients that are not within the prefix in the second affinity definition, the ServerIron ADX uses the default affinity definition. The ServerIron ADX sends clients whose IP addresses are within the 192.108.22.0/22 prefix to a VIP on slb-1 at the "atlanta" site, when available. The ServerIron ADX sends all other clients to a VIP on slb-1 at the "sunnyvale" site when available.

Displaying RTT prefix cache entries

You can display RTT prefix cache entries. The GSLB ServerIron ADX maintains a cache of RTT information received from the site ServerIron ADXs through the GSLB protocol. You can display the RTT information the GSLB ServerIron ADX has related to a client IP address.

To display affinity configuration information, enter the following command at any level of the CLI.

```
ServerIronADX(config)# show gslb cache 192.108.22.0
prefix length = 22, prefix = 192.108.22.0, region = N-AM
prefix source = affinity, client-query
affinity = site: atlanta, ServerIronADX: 192.108.22.111 slb-1

www.brocade.com:
  site = atlanta,  ServerIronADX = slb-1(192.108.22.111),  rtt = 4 (x100 usec)
```

Syntax: **show gslb cache** *<ip-addr>*

The *<ip-addr>* command specifies a site address.

The output in this example shows the information in the GSLB ServerIron ADX's prefix cache for prefix 192.108.22.0, including the affinity configuration information.

The prefix source field indicates the source of the prefix. If the source is "affinity", the prefix is associated with a site ServerIron ADX as part of an affinity definition.

If the ServerIron ADX contains an affinity definition for the prefix you specify, the affinity information is listed in the affinity field. The affinity field indicates the GSLB site, management IP address, and GSLB name of the ServerIron ADX associated with the prefix.

Displaying affinity selection counters

You can display the number of times an IP address is selected based on affinity. To display the information, enter the following command.

```
ServerIronADX(config)# show gslb dns detail
ZONE: gslb.com
HOST: www:
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*       1.1.1.101: dns v-ip    ACTIVE N-AM      0    0     4 (100%)
                  site: santaclara, ServerIronADX: 1.1.1.102
                  session util:   0%, avail. sessions: 5999988
                  preference: 128
                  Metric counter (count [selection-metric]):
                  3[health-check]
                  Affinity selection count = 1

*       1.1.1.115: dns real-ip DOWN   N-AM     --   --    0 (0%)
```

In the example, IP address 1.1.1.101 has been selected a total of four times as the best IP address; it has been chosen three times based on the health check metric and once based on affinity as displayed through the Affinity selection count.

Syntax: **show gslb dns detail** [<*name*>]

The <*name*> parameter specifies a zone name.

GSLB domain-level affinity

This section contains the following sections:

- "Overview of GSLB domain-level affinity" on page 88
- "Command line interface" on page 89

Overview of GSLB domain-level affinity

Users need the flexibility to associate a different set of affinities with different domains. For instance, user may want to direct all traffic from 199.239.0.0/24 subnet to ServerIron ADX A for domain *www.times.com* but not for another domain *www.travel.com* configured on the same controller. User cannot implement this using the existing global affinity definitions which apply to all the domains.

This document describes a feature called domain-level affinity which will allow the user to configure domain-level affinity groups and associate these with the desired domains. As a result, user has the flexibility of specifying different affinities for different domains. We will continue to support global affinity. We will support 128 domain-level affinity groups. Each domain-level affinity group can contain different number of affinity definitions as needed but the total number of affinity definitions across all the groups including global affinity cannot exceed 1024. User may also use all the 1024 entries just for global affinity definitions or domain-level affinity definitions. User can associate a domain-level affinity group with multiple domains. Only one domain-level affinity group can be associated with a domain.

Command line interface

Users will now be able to configure domain-level affinity groups in addition to the global affinity definitions. The new command line interface for the domain-level affinity feature is described below.

Creating a domain-level affinity group

To create a domain-level affinity group, use the following commands.

```
ServerIronADX(config)#gslb affinity-group 1
ServerIronADX(config-gslb-affinity-group-1)#
```

Syntax: [no] **gslb affinity-group** <*group-number*>

- <*group-number*>—specifies the group number

Specifying affinities definitions for the domain-level affinity group

To specify the affinities for the domain-level affinity group, use the following commands.

```
ServerIronADX(config)#gslb affinity-group 1
ServerIronADX(config-gslb-affinity-group-1)# prefer 1.1.1.102 for 1.1.1.0/24
ServerIronADX(config-gslb-affinity-group-1)# prefer 2.1.1.1 for 2.1.0.0/16
```

Syntax: [no] **prefer** <*site-name*> <*si-name*> | <*si-ip-addr*> **for** <*ip-addr*> <*ip-mask*> | <*ip-addr*>/<*prefix-length*>

Configuring an affinity for prefix 0.0.0.0/0

To configure an affinity for a ServerIron ADX for prefix 0.0.0.0/0, use the following commands.

```
ServerIronADX(config)#gslb affinity-group 1
ServerIronADX(config-gslb-affinity-group-1)# prefer 1.1.1.102 for 1.1.1.0/24
ServerIronADX(config-gslb-affinity-group-1)# prefer 2.1.1.102 for 0.0.0.0/0
```

When this group is associated with a domain, all clients from subnet 1.1.1.0/24 querying for this domain are directed to ServerIron ADX 1.1.1.102. All other client subnets querying for this domain are directed to ServerIron ADX 2.1.1.102.

Associating the domain-level group with a domain

To associate a domain-level affinity group with a domain, use the following commands.

```
ServerIronADX(config)# gslb dns zone gslb.com
ServerIronADX(config-gslb-dns-gslb.com)# host www http
ServerIronADX(config-gslb-dns-gslb.com)# host www affinity-group 1
```

Syntax: **host-info** <*host-name*> **affinity-group** <*group-number*>

- The <*host-name*> parameter specifies the host name.
- The <*group-number*> parameter is the group number of the domain-level affinity group being associated with this domain

NOTE
You have to configure the domain-level affinity group before you can associate it with the domain.

Show commands

- "show gslb affinity-group <group-number>"
- "show gslb resources"
- "show gslb dns zone"
- "show gslb dns detail"

show gslb affinity-group <*group-number*>

Use this command to display the affinity group, associated affinity definitions, and other related information.

Syntax: show gslb affinity-group [<*group-number*>]

If no group number is specified, this command displays all the domain affinity groups.

```
ServerIronADX# show gslb affinity-group 1
 gslb affinity-group 1
  pref 3.3.3.3 for 3.3.3.0/24
```

show gslb resources

Use this command to display the current and maximum number of affinity definitions in the global and domain-level affinity groups.

Syntax: show gslb resources

```
ServerIronADX# show gslb res

GSLB resource usage:
                    Current   Maximum
sites               3         128
SIs                 3         200
SIs' VIPs           2         2048
dns zones           1         1000
dns hosts           1         1000
health-checks app.  1         1000
dns IP addrs.       2         2048
affinities          3         1024
affinity groups     3         128
static prefixes     0         250
user geo prefixes   0         512
prefix cache        108       101024
RTT entries         0         50000
GSLB host policies  0         100
```

show gslb dns zone

Use this command to display the affinity group associated with the domain.

Syntax: show gslb dns zone [<*zone-name*>]

```
ServerIronADX# show gslb dns zone

ZONE: foo.com
HOST: www:
(Global GSLB policy)
GSLB affinity group: 7
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*        1.1.1.16: cfg real-ip ACTIVE N-AM      5   17    0 (0%)
*       1.1.1.108: cfg v-ip    ACTIVE N-AM      0    0    5 (100%)
```

show gslb dns detail

Use this command to display the affinity group associated with the domain and the number of selections based on affinity.

Syntax: **show gslb dns detail** [<*zone-name*>]

```
ServerIronADX# show gslb dns detail

ZONE: foo.com
HOST: www:
(Global GSLB policy)
GSLB affinity group: 7
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*        1.1.1.16: cfg real-ip ACTIVE N-AM      5   15    0 (0%)
*       1.1.1.108: cfg v-ip    ACTIVE N-AM      0    0    5 (100%)
                  Active Bindings: 1
                  site: local, weight:   0, SI: 1.1.1.102
                  session util:   0%, avail. sessions: 1999996
                  preference: 128
                  Metric counter (count [selection-metric]):
                  No metric count yet
                  Affinity selection count = 5
```

Debug command

Use the following command to enable debugging for domain-level affinity.

```
ServerIronADX(config)# gslb trace 10
```

Syntax: **gslb trace** [<*decimal*> | <*help*>]

DNS cache proxy

The DNS cache proxy feature allows the ServerIron ADX to act as a proxy for a DNS server by responding directly to the client queries without forwarding them to the DNS server. Just as in the GSLB DNS proxy mode, the ServerIron ADX periodically queries the authoritative DNS server for IP addresses corresponding to the domains configured for GSLB and caches them. However, unlike GSLB DNS proxy, the ServerIron ADX does not forward every client query to the authoritative DNS server, it responds directly to the client using the cached address list for the requested domain.

When you enable DNS cache proxy, the ServerIron ADX applies the GSLB policy to the IP addresses it has cached for the requested domain, and responds to the client with the best address. The ServerIron ADX refreshes the address cache by periodically querying the authoritative DNS server. The default update interval is 30 seconds and is configurable.

The DNS cache proxy feature is useful in network environments where the traffic between the ServerIron ADX and the authoritative DNS server introduces noticeable latency in the response to client requests. For example, if the ServerIron ADX and the authoritative DNS server are connected over the Internet, this feature can eliminate the delays caused by that connection.

In configurations where the ServerIron ADX and DNS server are co-located, the additional round trip time between the ServerIron ADX and DNS server is usually negligible. However, if the ServerIron ADX and DNS server are in different networks, the delay can become significant. In this case, the DNS cache proxy can help enhance performance by eliminating the exchange between the ServerIron ADX and DNS server for responses to client queries.

The DNS cache proxy feature is disabled by default. When the feature is disabled, the ServerIron ADX forwards client requests to the actual DNS server, applies the GSLB policy to the responses, then sends the optimized response to the client. In this case, the round trip time between the ServerIron ADX and DNS server is part of the overall round trip time between when the client sends the request and when the client receives the response.

If the GSLB ServerIron ADX cannot respond directly to the client for the requested domain (for example, because the domain is not configured on the GSLB ServerIron ADX), the ServerIron ADX sends the request through to the DNS server. This is the same behavior as when the DNS cache proxy feature is disabled.

NOTE
You can combine the DNS cache proxy feature with the DNS override feature (added in software release 06.0.03) to completely eliminate the separate DNS server. In this case, the ServerIron ADX contains all the required DNS information. Refer to "Combining the DNS cache proxy and DNS override features" on page 94.

Enabling DNS cache proxy

To enable DNS cache proxy, enter the following commands.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns cache-proxy
```

Syntax: [no] dns cache-proxy

Displaying DNS cache proxy state

To display the current GSLB policy settings, which include the DNS cache proxy state, enter the following command at any level of the CLI.

```
ServerIronADX(config)# show gslb policy
  Default metric order: ENABLE
  Metric processing order:
                1-Server health check
                2-Remote ServerIronADX's session capacity threshold
                3-Round trip time between remote ServerIronADX and client
                4-Geographic location
                5-Remote ServerIronADX's available session capacity
                6-Server flashback speed
                7-Least response selection

  DNS active-only: DISABLE  DNS best-only: DISABLE  DNS override: DISABLE
  DNS cache-proxy: ENABLE   DNS transparent-intercept: DISABLE
```
remaining rows omitted for brevity...

Syntax: show gslb policy

The command output shown in bold type in the example indicates the DNS cache proxy state. The state can be one of the following:

- DISABLE (the default)
- ENABLE

Displaying DNS cache proxy statistics

The GSLB ServerIron ADX maintains statistics for the transparent DNS as well as DNS proxy mode query intercept and DNS cache proxy features.

The following statistics are displayed for DNS cache proxy:

- Number of DNS queries the GSLB ServerIron ADX has responded to using the DNS cache proxy feature instead of forwarding the queries to the DNS server. (See the Direct response field under “DNS cache proxy stat:” in the output.)

The following statistics are displayed for transparent DNS query intercept:

- Number of queries the ServerIron ADX has redirected to a proxy DNS server or another ServerIron ADX. (See the Redirect field under “DNS query intercept stat:” in the output.)
- Number of queries to which the ServerIron ADX has directly responded using a transparent DNS query intercept IP address configured on the ServerIron ADX itself. (See the Direct response field under “DNS query intercept stat:” in the output.)

NOTE

The counter displayed from the **show gslb global-stat** command are maintained differently on the Management and BP consoles. On the Management console the counts are aggregated from all BPs. On the BP console the count displayed os only for the BP being accessed.

To display DNS cache proxy statistics, enter the following command at any level of the CLI.

```
ServerIronADX(config)# show gslb global-stat
DNS cache proxy stat:
Direct response      =         10

DNS query intercept stat:
Redirect             =          0  Direct response      =          0

ServerIronADX# show gslb global-stat

DNS cache proxy stat:

Direct response      =          4


DNS query intercept stat:

Redirect             =          0  Direct response      =          0


Unsupported query types stat:

Error handling cnt   =          0
```

Syntax: **show gslb global-stat**

The Direct response field, under “DNS cache proxy stat”, lists how many DNS queries the GSLB ServerIron ADX has responded to using the DNS cache proxy feature instead of forwarding the queries to the DNS server. In this example, the GSLB ServerIron ADX has responded directly to client queries ten times with the best site address among those cached on the ServerIron ADX itself, instead of forwarding the request to the DNS server.

For information about the statistics in the DNS query intercept stat section, refer to “Displaying transparent DNS query intercept statistics” on page 101.

Combining the DNS cache proxy and DNS override features

When the DNS cache proxy feature is enabled, the GSLB ServerIron ADX has to query the authoritative DNS server at regular intervals, to refresh the IP address list for each domain configured for GSLB. You can eliminate the need for a backend DNS server, by combining the cache proxy feature with the DNS override feature.

When you enable the DNS override feature, you also need to configure an IP list for the required domains. The ServerIron ADX performs health checks on the IP addresses configured for the domains and directly responds to client queries by using the GSLB policy to select the best IP address from the IP list configured for the requested domain.

By combining the DNS cache proxy feature with the DNS override feature, you can configure the ServerIron ADX to directly respond to client requests, without ever consulting the authoritative DNS server.

NOTE
A GSLB ServerIron ADX does not contain all the features of a real DNS server and thus cannot completely replace the DNS server.

NOTE
Although you do not need a real DNS server when you combine DNS cache proxy with DNS override, you still need to configure a virtual IP address for the DNS server. Clients send queries to the virtual IP address.

For information about configuring DNS cache proxy, refer to “DNS cache proxy” on page 91. For information about configuring DNS override, see “Enabling DNS override” on page 33.

To add a virtual IP address to which the clients can send their DNS queries, enter a command such as the following:

```
ServerIronADX(config)# server virtual-name-or-ip dns-proxy 209.157.23.87
ServerIronADX(config-vs-dns-proxy)# port dns
```

The command in this example adds IP address 209.157.23.87 as a virtual server. When clients send their DNS queries to this address, the ServerIron ADX processes the queries.

GSLB DNS type any query

DNS servers perform the translation between fully qualified domain names and IP addresses. DNS supports a number of record types such as IPv4 Address records (A records), IPv6 Address records (AAAA records), Name Server records (NS records), Mail Exchange (MX records), Canonical Name records (CNAME records) and so on.

GSLB ServerIron ADX performs GSLB on client queries for IPv4 address records (A records). In GSLB topologies, when the client query comes in for any of the other record types, the GSLB ServerIron forwards the query to the backend DNS server and sends the DNS response unaltered to the client.

DNS supports a special query type called "ANY". If the client sends a DNS query with type ANY, the DNS response contains all the records configured for that domain. For example, if two A records and two MX records are configured for *www.mycompanynet.com* and the client sends a type ANY query for *www.mycompanynet.com*, then the DNS response contains all four records: two A records and two MX records.

GSLB ServerIron ADX is able to handle DNS type ANY queries. If the client sends a DNS query with type ANY, GSLB ServerIron ADX identifies it as a supported query type and performs GSLB on the A records contained in the response.

In modes such as DNS proxy, when client sends a query with DNS type ANY, GSLB ServerIron ADX receives the DNS server response containing all the DNS records configured for the domain. In addition to query type A records, GSLB ServerIron ADX also identifies type ANY as a supported query type. It will parse the DNS response to find all the A records contained within the response. It will apply the GSLB policy to this response, reorder the A records in the response with the best A record at the top and send the response to the querying client. Note that all records other than A records (such as MX records and others) contained within the response, are not changed by the GSLB ServerIron ADX.

In modes such as DNS cache proxy with DNS override, the GSLB ServerIron ADX does not have a backend DNS server and generates the DNS response itself. If client sends a query of type ANY, GSLB ServerIron ADX will identify this as a supported query type and apply the GSLB policy to the IP addresses for the domain. It will send a response to the client with the selected A record for the domain.

This feature is enabled by default.

Transparent DNS query intercept

Transparent DNS query intercept allows a ServerIron ADX to transparently intercept certain DNS queries to the authoritative DNS server and redirect them to alternate DNS servers or handle them directly. This feature lets the authoritative DNS server IP remain unchanged. You do not need to change the DNS server IP address as you do in standard GSLB configurations.

This feature is useful when you want to redirect clients for certain domains to proxy web servers, but you do not want to configure the proxy addresses on the DNS server itself or otherwise change the configuration of the DNS server.

NOTE
The ServerIron ADX must be in the direct data path from all potential clients to the authoritative DNS server. Otherwise, it is possible for the DNS server to receive the queries directly instead of the ServerIron ADX.

You can configure the following types of transparent DNS query intercept:

- Redirect the client queries to a proxy DNS server and perform GSLB on the response. The ServerIron ADX redirects the client request for the zones configured on the ServerIron ADX to the alternate DNS server, applies the GSLB policy on the response and gives the best address(es) to the client.

- Redirect the client queries to a proxy DNS server and send the reply unchanged. The ServerIron ADX redirects the client request to the alternate DNS server and sends the response, as is, to the client. The alternate DNS server could be a ServerIron ADX configured for GSLB, in which case the reply has the best address(es) for the client.
- Directly respond to client queries using the IP addresses configured for the domain. The ServerIron ADX does not forward or redirect the query to the actual or proxy DNS servers. Instead, it directly responds to the client by applying GSLB policy to pick the best IP address from among the IP list configured for the domain.

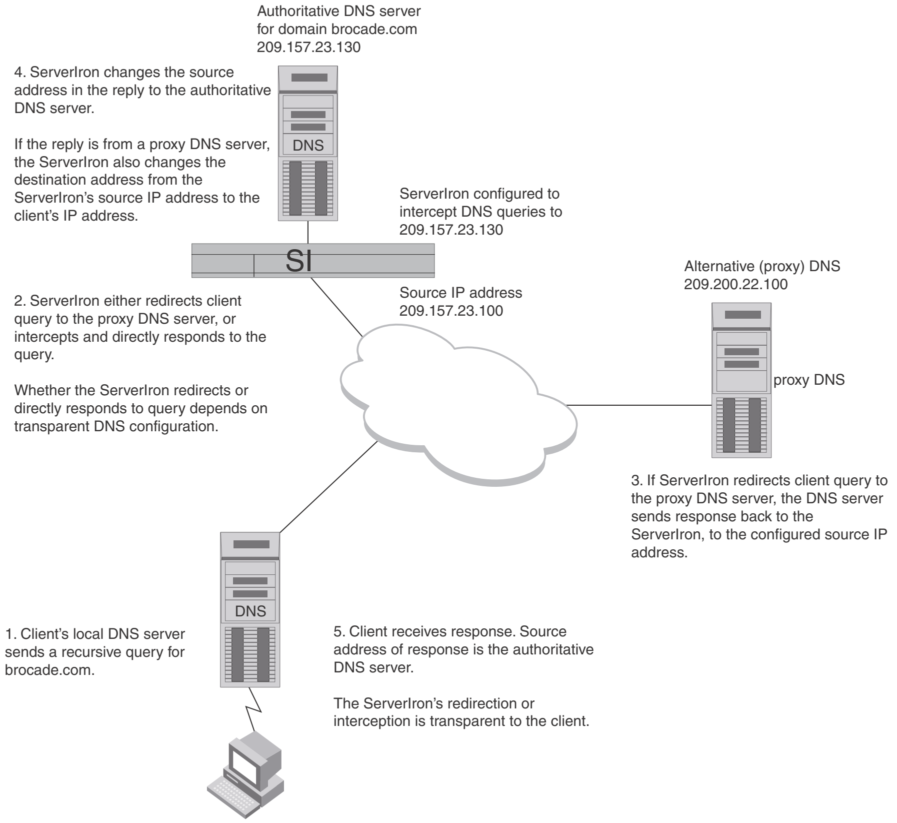
NOTE
A ServerIron ADX configured for transparent intercept redirects or directly responds to client requests only for domain configured on the ServerIron ADX. If the domain name requested by the client is not configured on the ServerIron ADX, it forwards the query to the actual DNS server without intercepting, and the reply is untouched by GSLB.

Example

Figure 6 shows an example of a configuration that uses transparent DNS query intercept. In this example, the ServerIron ADX is configured to intercept all client queries to the zone brocade.com and redirect them to the proxy DNS server and apply GSLB on the reply. The ServerIron ADX uses its configured source-ip to make sure the DNS reply from the proxy server comes to it.

- The client's local DNS server sends a recursive query for brocade.com to the authoritative DNS server (209.157.23.130).
- The ServerIron ADX intercepts and redirects client query to proxy DNS server (209.200.22.100).
- The proxy DNS server sends response back to the ServerIron ADX's source IP address (209.157.23.100).
- The ServerIron ADX changes the source address in the reply to the authoritative DNS server's address and the destination address from the ServerIron ADX's source-IP to the client's IP address.
- The client receives the DNS response with the authoritative DNS server's source IP address. The ServerIron ADX's interception and redirection is transparent to the client.

FIGURE 6 Transparent DNS query intercept configuration


Authoritative DNS server
for domain brocade.com
209.157.23.130
4. ServerIron changes the source address in the reply to the authoritative DNS server.
If the reply is from a proxy DNS server, the ServerIron also changes the destination address from the ServerIron's source IP address to the client's IP address.
DNS
ServerIron configured to intercept DNS queries to 209.157.23.130
SI
Alternative (proxy) DNS
209.200.22.100
2. ServerIron either redirects client query to the proxy DNS server, or intercepts and directly responds to the query.
Whether the ServerIron redirects or directly responds to query depends on transparent DNS configuration.
Source IP address
209.157.23.100
proxy DNS
3. If ServerIron redirects client query to the proxy DNS server, the DNS server sends response back to the ServerIron, to the configured source IP address.
DNS
1. Client's local DNS server sends a recursive query for brocade.com.
5. Client receives response. Source address of response is the authoritative DNS server.
The ServerIron's redirection or interception is transparent to the client.

Redirecting queries

To configure transparent DNS query intercept to redirect queries to a proxy DNS server or another GSLB ServerIron ADX:

- Configure a real server with the IP address of the proxy DNS server or other GSLB ServerIron ADX to which you want to redirect queries.
- Configure a virtual server with the IP address of the authoritative DNS server that you want to intercept.
- Specify the domain and host application for which you want to intercept queries.
- Configure an IP policy to enable the ServerIron ADX to examine incoming DNS packets.

NOTE
In standard GSLB configuration, the ServerIron ADX sends a DNS query to the DNS server to get the IP addresses for the domain and performs health-checks on them. However in this transparent intercept mode, where you do not do GSLB on the DNS response, the ServerIron ADX does not do these things.

NOTE
The ServerIron ADX intercepts queries only for domain names configured on the ServerIron ADX. For domain names that are not configured on the ServerIron ADX, the ServerIron ADX still sends queries to the authoritative DNS server.

Use the following CLI method to configure this feature.

To configure the ServerIron ADX to redirect queries to an alternative DNS server, enter commands such as the following:

```
ServerIronADX(config)# source-ip 209.157.23.100 255.255.255.0 0.0.0.0
ServerIronADX(config)# server remote-name dns-redirect 209.200.22.100
ServerIronADX(config-rs-dns-redirect)# source-nat
ServerIronADX(config-rs-dns-redirect)# port dns
ServerIronADX(config-rs-dns-redirect)# exit
ServerIronADX(config)# server virtual-name-or-ip dns-intercept 209.157.23.130
intercept
ServerIronADX(config-vs-dns-intercept)# port dns
ServerIronADX(config-vs-dns-intercept)# bind dns dns-redirect dns
ServerIronADX(config-vs-dns-intercept)# exit
ServerIronADX(config)# gslb dns zone brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# exit
```

Syntax: [no] server source-ip *<ip-addr> <ip-mask> <default-gateway>*

NOTE
The gateway parameter is required. If you do not want to specify a gateway, enter "0.0.0.0".

This command adds a source IP address. The ServerIron ADX uses the source IP address in packets that it sends to the alternative DNS server (the "real server"). Add an address that is in the same subnet as the ServerIron ADX's management IP address. If you do not add a source IP address and enable source NAT, the ServerIron ADX leaves the client's IP address in the source address field of the redirected IP packets and as a result may not receive the alternative DNS server's responses. The ServerIron ADX needs to receive the responses so it can modify the source IP address to match the address of the authoritative DNS server, so that when the client receives the response, the response appears to be from the authoritative DNS server. The redirection is thus transparent to the client.

Syntax: [no] server remote-name *<name> <ip-addr>*

This command adds the alternative DNS server (the one to which you want to redirect queries). You can enter this command multiple times for multiple alternative DNS servers.

NOTE
You can configure the alternate DNS server as a real server if it is in the same subnet as the ServerIron ADX.

Syntax: [no] source-nat

This command enables source NAT. Source NAT allows the ServerIron ADX to change the source IP address in the client request to one of the source addresses configured on the ServerIron ADX. You must configure a source IP address and enable source NAT. You can enable source NAT globally or on individual real servers (as in the example above).

Syntax: [no] port dns

This command enables the DNS port on the real server. You must use this command so that the ServerIron ADX knows you want to redirect DNS traffic to the real server (the alternative DNS server).

Syntax: [no] server virtual-name-or-ip *<name> <ip-addr>* intercept

This command configures a virtual server that has the DNS server's actual IP address. When the ServerIron ADX receives a DNS query addressed to the DNS server IP address, the ServerIron ADX intercepts the packet instead of forwarding it to the DNS server. The **intercept** parameter is required and indicates that you want to use the virtual server for intercepting DNS queries. This parameter also instructs the ServerIron ADX to ignore ARP requests and pings to the address. The ServerIron ADX needs to ignore ARPs and pings to the address because the address still belongs to the authoritative DNS server. Without the intercept parameter, the ServerIron ADX will respond to ARPs and pings to the virtual server's IP address.

Syntax: **[no] bind dns** <*real-server-name*> **dns**

This command binds the real server (the alternative DNS server) to the virtual server (the intercepted authoritative DNS server). This command creates an entry in the ServerIron ADX's port binding table that allows the ServerIron ADX to redirect DNS traffic sent to the authoritative DNS server to the alternative DNS server.

Syntax: **[no] gslb dns zone-name** <*name*>

This command specifies the zone for which you want to intercept queries. The ServerIron ADX will intercept and redirect DNS queries only for the zones you specify, and forwards all other client queries to the authoritative DNS server.

Syntax: **[no] host-info** <*host-name*> <*host-application*> **|** <*tcp/udp-portnum*>

This command specifies the host application on the zone you specified above.

Syntax: **ip policy** <*index*> **cache udp dns global**

This command enables the ServerIron ADX to examine incoming DNS packets. This command is required.

Redirecting queries and perform GSLB

To configure transparent DNS query intercept to redirect queries to a proxy DNS server and perform GSLB on the response, do the following:

- Configure a real server with the IP address of the proxy DNS server
- Configure a virtual server with the IP address of the authoritative DNS server, which you want to intercept.
- Specify the domain and host application for which you want to intercept queries.
- Configure an IP policy to enable the ServerIron ADX to examine incoming DNS packets.
- Enable port dns proxy on the real server corresponding to the proxy server.

NOTE
A ServerIron ADX intercepts queries only for domain names configured on the ServerIron ADX. For domain names that are not configured on a ServerIron ADX, the ServerIron ADX still sends queries to the authoritative DNS server.

To configure the ServerIron ADX to redirect queries to another DNS server and apply GSLB on the response, enter commands such as the following:

```
ServerIronADX(config)# source-ip 209.157.23.100 255.255.255.0 0.0.0.0
ServerIronADX(config)# server remote-name dns-redirect 209.200.22.100
ServerIronADX(config-rs-dns-redirect)# source-nat
ServerIronADX(config-rs-dns-redirect)# port dns proxy
ServerIronADX(config-rs-dns-redirect)# exit
ServerIronADX(config)# server virtual-name-or-ip dns-intercept 209.157.23.130
intercept
ServerIronADX(config-vs-dns-intercept)# port dns
ServerIronADX(config-vs-dns-intercept)# bind dns dns-redirect dns
ServerIronADX(config-vs-dns-intercept)# exit
ServerIronADX(config)# gslb dns zone brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# exit
```

The commands are the same as the ones for configuring the ServerIron ADX to redirect queries directly to another DNS server, with one difference. The command that enables the DNS port on the real server (the other ServerIron ADX) uses the **proxy** parameter. This parameter indicates that the ServerIron ADX needs to perform GSLB on the response before sending the response back to the client.

Responding to queries directly

To configure transparent DNS query intercept to directly respond to queries using IP addresses configured on the ServerIron ADX, do the following:

- Configure a virtual server with the IP address of the authoritative DNS server that you want to intercept.
- Specify the domain name and host application for which you want to intercept queries.
- Enable the DNS transparent intercept feature.
- Configure an IP policy to examine incoming DNS packets.
- Enable **dns transparent-intercept** in the GSLB policy.

NOTE
In the direct-response mode, the ServerIron ADX uses GSLB to pick the best address by default. No additional configuration is needed to further enable GSLB.

NOTE
The ServerIron ADX intercepts queries only for domain names configured on the ServerIron ADX. For domain names that are not configured on the ServerIron ADX, the ServerIron ADX still sends queries to the authoritative DNS server.

To configure the ServerIron ADX to respond to queries using a set of IP addresses configured on the ServerIron ADX itself, enter commands such as the following:

```
ServerIronADX(config)# server virtual-name-or-ip dns-intercept 209.157.23.130
intercept
ServerIronADX(config-vs-dns-intercept)# port dns
ServerIronADX(config-vs-dns-intercept)# gslb dns zone brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# host-info www ip-list 209.200.1.1
209.200.1.2 209.200.1.3 209.200.1.4 209.200.1.5
ServerIronADX(config-gslb-dns-brocade.com)# exit
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns transparent-intercept
```

These commands configure a virtual server for the authoritative DNS server IP address, specify the zone and host names for which to intercept queries, and specify the IP addresses to use in responses to the queries. The commands also enable the DNS transparent intercept feature and enable the ServerIron ADX to examine incoming DNS packets.

NOTE
For non-direct respond transparent intercept, you should not enable **dns transparent-intercept** in the **gslb policy.**

Notice that unlike the types of transparent DNS query intercept shown in “Redirecting queries” on page 97, the type shown here does not require configuration of a real server. Since the ServerIron ADX in this case is responding directly to the query instead of redirecting the query to another device, only the virtual server for intercepting the queries is required. Moreover, since the ServerIron ADX is not redirecting the queries, you do not need to configure a source IP address and enable source NAT.

Syntax: host-info <*host-name*> **ip-list** { <*ipv4-address*> | <*ipv6-address*> }

This command specifies the IPv4 or IPv6 addresses you want the ServerIron ADX to use in its replies to the intercepted DNS queries. You can specify as many addresses as you need. Separate each address with a space.

The ServerIron ADX applies the GSLB policy to the addresses and sends only the best address in the response to a client query. If the GSLB policy does not result in a best address to send to the client, the ServerIron ADX forwards the request to the authoritative DNS server. In either case, the source IP address in the response is the DNS server IP address, so the client always receives a response that appears to be from the DNS server.

Syntax: dns transparent-intercept

This command enables the DNS transparent intercept feature. You need to use this command only when you are configuring the type of transparent DNS query intercept that responds directly to the client. If you are configuring the type of transparent DNS query intercept that redirects the query to an alternative DNS server or to another ServerIron ADX, do not use this command.

For information about the other commands, refer to “Redirecting queries” on page 97.

Displaying transparent DNS query intercept statistics

To display transparent DNS query intercept statistics, enter the following command at any level of the CLI.

```
ServerIronADX(config)# show gslb global-stat

DNS cache proxy stat:
Direct response      =          0

DNS query intercept stat:
Redirect             =          0  Direct response      =          0

Unsupported query types stat:
Error handling cnt   =          0
```

Syntax: show gslb global-stat

The transparent DNS query intercept statistics are displayed in the DNS query intercept stat section.

TABLE 7 Transparent DNS query intercept statistics

This field...	Displays...
Redirect	The number of queries the ServerIron ADX has redirected to an alternative (proxy) DNS server or another ServerIron ADX.
Direct response	The number of queries to which the ServerIron ADX has directly responded using an IP address configured for the domain.

For information about the statistics in the DNS cache proxy stat section, refer to “Displaying DNS cache proxy statistics” on page 93.

Enabling DNS request logging

You can enable logging of the following information for DNS requests assisted by the GSLB ServerIron ADX:

- Source IP address (the address of the client making the request)
- Best IP address (site address provided by the ServerIron ADX)
- Host
- Zone
- Metric used

When you enable logging of this information, the ServerIron ADX generates a syslog message for each DNS requests assisted by the ServerIron ADX.

NOTE
The ServerIron ADX sends the log messages only to the external syslog servers you have configured on the ServerIron ADX. The messages do not appear in the ServerIron ADX’s syslog buffer.

To enable logging of request information, enter the following command at the global CONFIG level of the CLI.

```
ServerIronADX(config)# gslb log-dns
```

Syntax: [no] gslb log-dns

Here are some examples of the messages generated by this feature. In this example, client 1.1.1.21 sends four requests for *www.gslb.com*.

```
20:52:02  User.Info 1.1.1.102  GSLB DNS request: src-ip = 001.001.001.021  best-ip
= 001.001.001.101  Host = www  Zone = gslb.com  Metric = health-check
20:51:54  User.Info 1.1.1.102  GSLB DNS request: src-ip = 001.001.001.021  best-ip
= 001.001.001.101  Host = www  Zone = gslb.com  Metric = least-response
20:51:54  User.Info 1.1.1.102  GSLB DNS request: src-ip = 001.001.001.021  best-ip
= 001.001.001.023  Host = www  Zone = gslb.com  Metric = least-response
20:51:53  User.Info 1.1.1.102  GSLB DNS request: src-ip = 001.001.001.021  best-ip
= 001.001.001.022  Host = www  Zone = gslb.com  Metric = least-response
```

Each message shows the following information.

TABLE 8 GSLB request information

This field...	Displays...
User.Info	The management IP address of the GSLB ServerIron ADX.
src-ip	The IP address of the client that sent the DNS request.
best-ip	The IP address selected by the GSLB ServerIron ADX as the best site.
Host	The host application requested by the client.
Zone	The zone name requested by the client.
Metric	The GSLB metric according to which the site was selected as the best site.

Support for the RTT metric

When GSLB ran on the MP, the controller cached an RTT update only if that particular IP address had made a DNS query earlier. This was to eliminate unnecessary RTT entries in the controller's local cache. When a client made a DNS request, the controller cached the client's prefix, as well as the hostname it queried, in its local cache for a period of time, two minutes by default. The controller stored the RTT update from the GSLB agent for a client network only if the client had previously requested a domain name.

This behavior cannot be carried over to multiple CPUs because the BP that serves the DNS request has to notify the other CPUs about the client's request. The other CPUs can then cache the RTT update, being well aware that a client from that network had made a DNS query already. This means each DNS query would result in an IPC message, which is not acceptable for performance reasons.

The client prefix entry is created when a site sends an RTT update for the client network. The cache entry has a default age value of two minutes, which is refreshed each time a client from that network makes a DNS query, or if a site sends an RTT update for that client's network. In addition, the RTT cache organization was changed to become domain-name independent. Each client prefix points to a flat table consisting of GSLB sites against the client's RTT to the site. This is used to determine which IP address is best for a client by finding the site that is closest to the client, based on the RTT table.

This new design eliminates the limitation of storing only up to four proximity entries per domain name. Now as many RTT entries can be stored as there are sites configured on the controller.

The output of the **show gslb cache** command has been changed to accommodate these RTT changes. The following is sample output from the command. Note that the prefix entry has been created due to an RTT update from a site, and also that RTT entries for this client network from 6 different sites are cached. Previously, only the best four RTT entries were cached, no matter how many sites sent the updates.

```
ServerIronADX# show gslb cache 212.12.12.2
prefix length = 20, prefix = 212.12.0.0, region = EUROPE
prefix source = rtt-update,
  site = local,  ServerIron ADX = slb1(192.168.28.15),  rtt = 3 (x100 usec)
  site = client,  ServerIron ADX = slb1(192.9.1.1),  rtt = 4 (x100 usec)
  site = remote6,  ServerIron ADX = slb1(100.86.6.1),  rtt = 4 (x100 usec)
  site = remote7,  ServerIron ADX = slb1(192.168.7.1),  rtt = 6 (x100 usec)
  site = remote8,  ServerIron ADX = slb1(192.186.2.1),  rtt = 12 (x100 usec)
  site = remote9,  ServerIron ADX = slb1(192.19.3.1),  rtt = 8 (x100 usec)
```

BP support as GSLB agent

If the ServerIron ADX is used as a GSLB agent, the BP synchronizes RTT information collected from clients that make TCP SLB connections to the ServerIron ADX, to the MP. The MP communicates this RTT information to all collectors with which it opened TCP port 182 connections.

Note that the agent needs to be serving TCP SLB connections in order to collect RTT samples from client networks. This is because the ServerIron ADX bases the RTT calculation on the TCP 3-way handshake mechanism during connection establishment. If the agent is running only UDP applications, there will be no RTT updates from that agent.

Also note that the RTT is not application specific. All TCP connections are used to sample RTTs.

Distributed health checks for GSLB

The GSLB ServerIron ADX evaluates each IP address in the DNS reply based on a set of criteria. Depending on the results of this evaluation, the GSLB ServerIron ADX reorders the list to place the "best" IP address on the top of the list. Usually the GSLB ServerIron ADX uses a server's health as one of the most important criteria to evaluate the server IP addresses in a DNS reply. The GSLB distributed health check feature distributes the health checking task, currently carried out by the GSLB ServerIron ADX, to the site ServerIron ADXs.

A ServerIron ADX has the GSLB distributed health check feature enabled by default. If the GSLB ServerIron ADX as well as the site ServerIron ADX support the GSLB distributed health check feature, the site ServerIron ADX will periodically report the health check status information of the host servers being load balanced by it, to the GSLB ServerIron ADX. GSLB ServerIron ADX will no longer need to maintain health checks on these host servers being load balanced by this site ServerIron ADX. Thus the GSLB distributed health check feature helps offload the task of health checking from the GSLB ServerIron ADX and distributes it to the peer site ServerIron ADXs that support the GSLB distributed health check feature.

The distributed health check feature provides the following benefits:

- Reduction of GSLB ServerIron ADX load
- Reduction of GSLB health check traffic
- Increased scalability due to distribution of health checking task to site ServerIron ADXs
- Ability to configure and modify the interval at which site ServerIron ADXs report the health check information to the GSLB ServerIron ADX.

In addition to this, a distributed health check GSLB ServerIron ADX will inter-operate with a non-distributed health check site ServerIron ADX and a distributed health check site ServerIron ADX will also be compatible with a non-distributed health check GSLB ServerIron ADX (no additional configuration required). Some configuration is required in the first case but not the latter case. Refer to "Disabling the distributed health check feature for an individual site ServerIron ADX" on page 105 and "Disabling or re-enabling distributed health check" on page 106.

You are not required to use the same health check mode (distributed or centralized) on all ServerIron ADXs in the GSLB configuration. You can transition the distributed health check mechanism into your GSLB network, one site or even one site ServerIron ADX at a time, if desired. Alternatively, if you want to use the distributed health check feature for all ServerIron ADXs, all you need to do is upgrade all of them to 08.1.00S release.

The configuration required for the GSLB distributed health check feature depends on whether the GSLB ServerIron ADX and the site ServerIron ADX support the distributed health check feature or not. Refer to the table below for more information on the configuration available and mandated by the GSLB distributed health check feature.

	Site ServerIron ADX	
GSLB ServerIron ADX	**Distributed health check site ServerIron ADX**	**Non-distributed health check site ServerIron ADX**
Distributed health check GSLB ServerIron ADX	• No mandatory configuration required. • You can configure the health check status reporting interval. Refer to "Configuring the health status reporting interval" on page 106 and "Configuring the agent health report interval" on page 107. • Flashback metric disabled by default. Do not enable.	• Mandatory configuration required to disable distributed health check for this site ServerIron ADX. Refer to "Enabling the distributed health check feature for an individual site ServerIron ADX" on page 106 and "Disabling or re-enabling distributed health check" on page 106. • Flashback metric disabled by default. If you need to enable it, refer to "Impact of distributed health checks on the Flashback metric" on page 108 before doing so.
Non-distributed health check GSLB ServerIron ADX	• No configuration required. • Flashback metric enabled by default.	• Neither GSLB ServerIron ADX nor site ServerIron ADX is running the 08.1.00S release. Refer to the relevant release notes for information.

Disabling the distributed health check feature for an individual site ServerIron ADX

If a site ServerIron ADX does not support the distributed health check feature, and if the GSLB ServerIron ADX supports the distributed health check feature, then distributed health check feature should be disabled for that site ServerIron ADX as it does not support distributed health checking i.e. the GSLB ServerIron ADX still needs to maintain health checks for the host servers being load balanced by that site ServerIron ADX.

To disable distributed health check feature for an individual site ServerIron ADX, enter commands such as the following on the GSLB ServerIron ADX, not on the site ServerIron ADX.

```
GSLB-ServerIronADX(config)# gslb site sunnyvale
GSLB-ServerIronADX(config-gslb-site-sunnyvale)# si-name 1.1.1.107
no-si-dist-health-check
```

Syntax: [no] si-name [<*name*>] <*ip-addr*> no-si-dist-health-check

NOTE
The **si-name** command also has an optional parameter that specifies the ServerIron ADX's preference. This parameter is not related to the distributed health check feature.

Enabling the distributed health check feature for an individual site ServerIron ADX

You can enable the distributed health check feature for an individual site ServerIron ADX. Enter the commands such as the following on the GSLB ServerIron ADX, not on the site ServerIron ADX.

```
GSLB-ServerIronADX(config)# gslb site sunnyvale
GSLB-ServerIronADX(config-gslb-site-sunnyvale)# si-name abc 1.1.1.107
enable-si-dist-health-check
```

Syntax: [no] si-name [<*name*>] <*ip-addr*> enable-si-dist-health-check

Disabling or re-enabling distributed health check

You can disable the distributed health check feature for an entire GSLB site. When you do this, it applies to all the site ServerIron ADXs at that site. Note that if there is a configuration to enable or disable the distributed health check feature on an individual site ServerIron ADX (Refer to "Disabling the distributed health check feature for an individual site ServerIron ADX" on page 105 and "Enabling the distributed health check feature for an individual site ServerIron ADX" on page 106), the configuration on the individual ServerIron ADX takes effect for that site ServerIron ADX and overrides the site configuration for that site ServerIron ADX

To disable distributed health checks for a site, enter commands such as the following, enter the commands on the GSLB ServerIron ADX, not on the site ServerIron ADX:

```
GSLB-ServerIronADX(config)# gslb site sunnyvale
GSLB-ServerIronADX(config-gslb-site-sunnyvale)# no-distributed-health-check
```

Syntax: [no] no-distributed-health-check

To re-enable distributed health checks for the site, enter the following command.

```
GSLB-ServerIronADX(config-gslb-site-sunnyvale)# no no-distributed-health-check
```

Clearing the distributed health check settings for a site ServerIron ADX

You can clear the distributed health check settings for a site ServerIron ADX. When you clear the settings, the site ServerIron ADX inherits the settings configured for the site itself. (Refer to "Disabling or re-enabling distributed health check" on page 106.) If you have not configured distributed health check settings for the site, then the distributed health check feature is enabled for the site ServerIron ADX. This is the default setting for the feature.

To clear the distributed health check settings from a site ServerIron ADX, enter commands such as the following on the GSLB ServerIron ADX, not on the site ServerIron ADX.

```
GSLB-ServerIronADX(config)# gslb site sunnyvale
GSLB-ServerIronADX(config-gslb-site-sunnyvale)# si-name 1.1.1.107
clear-si-health-check-mech
```

Syntax: [no] si-name [<*name*>] <*ip-addr*>clear-si-health-check-mech

Configuring the health status reporting interval

If the GSLB ServerIron ADX supports the distributed health check feature, then you can globally configure the interval at which the distributed health check site ServerIron ADXs report the health check information to the GSLB ServerIron ADX for the GSLB distributed health check feature. Note that if health status interval is configured globally, it applies to all peer site ServerIron ADXs that support the distributed health check feature.

To globally configure the health status reporting interval, enter commands such as the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX(config)# gslb policy
GSLB-ServerIronADX(config-gslb-policy)# health-status-interval 3
```

Syntax: [no] health-status-interval <*secs*>

The <*secs*> parameter specifies the interval. Range is 2-120 seconds.

Configuring the agent health report interval

If both the GSLB ServerIron ADX and the site ServerIron ADX support the distributed health check feature, you can configure the interval at which the site ServerIron ADX reports the health check information to the GSLB ServerIron ADX for the GSLB distributed health check feature. To do this, enter a command such as the following:

```
SITE-ServerIronADX(config)# agent-health-report-interval 7
```

Syntax: [no] agent-health-report-interval <*secs*>

The <*secs*> specifies the interval. Range is 2-120 seconds.

This configuration can be made locally on the individual site ServerIron ADX. If health status reporting interval is also configured globally on the GSLB ServerIron ADX, then the health status interval configuration on the individual site ServerIron ADX takes precedence over it for that site ServerIron ADX. Note that if health status configuration is done neither globally on the GSLB ServerIron ADX nor locally on an individual site ServerIron ADX, then the site ServerIron ADX reports the health status information to the GSLB ServerIron ADX at default interval (i.e. every five seconds).

Debugging the distributed health check

You can debug the distributed health check feature on the GSLB controller ServerIron ADX, by enter a command such as the following on the GSLB controller ServerIron ADX.

```
GSLB-ServerIronADX# debug distributed-hcheck recvd-add-list
          GSLB:  recvd-add-list-event debugging is on
GSLB-ServerIronADX#Recvd add list msg from peer 192.9.1.1(len = 53)
Recvd add list msg from peer 192.9.1.17(len = 53)
```

This command displays “health check status report received” event. Whenever a health check status report is received from a site ServerIron ADX, a debug message is displayed on GSLB ServerIron ADX indicating the IP address of that ServerIron ADX as well as the length of that health check status report.

Syntax: debug distributed-hcheck recvd-add-list-event I sent-add-list

The **sent-add-list** option displays messages about “health check status report sent” events. When the site ServerIron ADX sends the health check status report to the peer GSLB ServerIron ADX, a debug message is displayed on the site ServerIron ADX indicating the VIPs that are a part of this health check status message. These messages help you determine if the site ServerIron ADX is sending the health check status report at the correct interval and with the correct VIPs.

To display messages about “health check status report sent” events, enter the following command on the site ServerIron ADX. T

```
SITE-ServerIronADX# debug distributed-hcheck sent-add-list
          GSLB:  sent-add-list debugging is on
SITE-ServerIronADX#
Sending Address List msg: VIP = 192.9.2.16, Active = 1, Host Range = 1, Num
Ports = 2
Sending Address List msg: VIP = 192.9.2.17, Active = 0, Host Range = 1, Num
Ports = 3
Sending Address List msg: done
```

Impact of distributed health checks on the Flashback metric

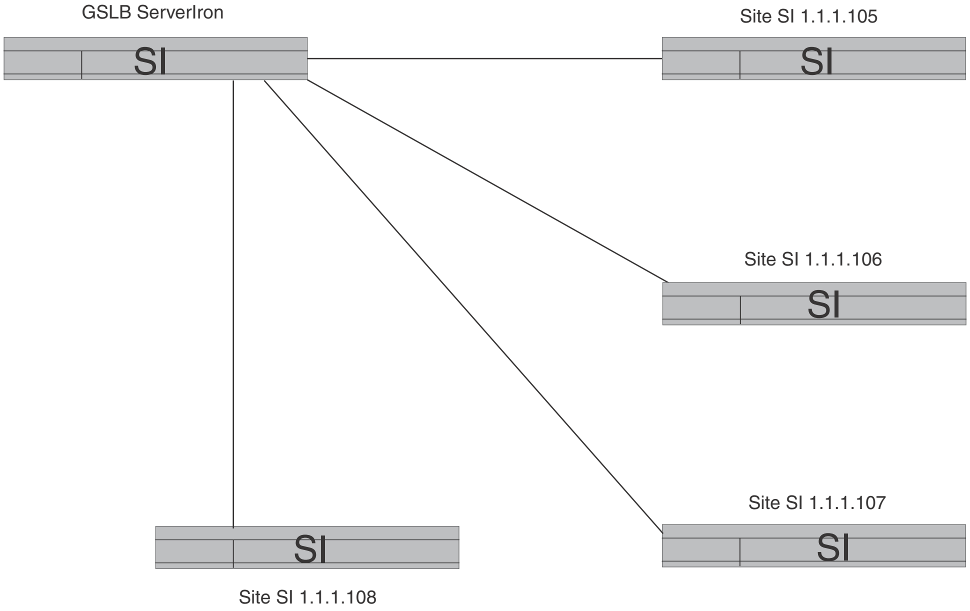
If the GSLB ServerIron ADX supports the distributed health check feature, then the Flashback metric is disabled by default in release 08.1.00S. Flashback is defined as the round-trip time for a health check sent by the GSLB ServerIron ADX to the host application on the server. Flashback delay is computed as the round-trip time of the Layer 4 health check to the TCP port and the round-trip time for the Layer 7 health check for the application. If the GSLB ServerIron ADX supports the distributed health check feature, then the Flashback metric is disabled by default. The reason for this is that the distributed health GSLB ServerIron ADX does not carry out health checks for the host servers load balanced by the distributed health check site ServerIron ADXs; instead the site ServerIron ADXs periodically report this health check status information to the GSLB ServerIron ADX. Note that the distributed health check GSLB ServerIron ADX still maintains health checks for the host servers behind the non-distributed health check site ServerIron ADXs. Thus the distributed health check GSLB ServerIron ADX maintains health checks and computes the Flashback delay only for host servers behind the non-distributed health check site Servers. Since Flashback delay is not relevant and not computed for all the host servers, the Flashback metric is disabled by default if the GSLB ServerIron ADX supports the distributed health check feature.

Flashback metric can be enabled on the distributed health check ServerIron ADX if required. This should be done with caution. You should enable the Flashback metric only if he or she is certain that all the peer site ServerIron ADXs support non-distributed health check only i.e. they do not support the distributed health check feature. In such a case, the health check for all of the host servers will be maintained by the GSLB ServerIron ADX and each of them will have an associated Flashback value.

NOTE
The Flashback delay value for the VIPs on site ServerIron ADXs that support the distributed health check feature will be displayed as “0” in the GSLB show commands. This implies that there is no Flashback delay value associated with that IP address.

Configuration examples

FIGURE 7 Topology



Example 1

In this example:

- The GSLB ServerIron ADX supports the distributed health check feature.
- Site ServerIron ADXs 1.1.1.105, 1.1.1.106 and ServerIron ADX 1.1.1.107 all belong to site “sunnyvale” and do not support the distributed health check feature.
- Site ServerIron ADX 1.1.1.108 belongs to site "santaclara" and supports the distributed health check feature.

Mandatory configuration is required to disable distributed health check for all ServerIron ADXs at site “sunnyvale” since none of the ServerIron ADXs at that site support the distributed health check feature.

Configure the following on the GSLB ServerIron ADX for site “sunnyvale”.

```
GSLB-ServerIronADX#conf t
GSLB-ServerIronADX(config)#gslb site sunnyvale
GSLB-ServerIronADX(config-gslb-site-sunnyvale)#no-distributed-health-check
GSLB-ServerIronADX(config-gslb-site-sunnyvale)#end
```

NOTE
You can also achieve the same result by individually disabling distributed health check for each ServerIron ADX at this site i.e. by disabling distributed health check individually for ServerIron ADX 1.1.1.105, ServerIron ADX 1.1.1.106 and ServerIron ADX 1.1.1.107, but it is simpler and more concise to just disable it for the whole site.

No mandatory configuration required for ServerIron ADX 1.1.1.108 as it supports the distributed health check feature.

In order to globally configure the health status interval to 7 seconds, configure the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX(config)# gslb policy
GSLB-ServerIronADX(config-gslb-policy)# health-status-interval 7
GSLB-ServerIronADX(config-gslb-policy)# end
```

The distributed health check ServerIron ADX 1.1.1.108 now starts sending the health check status information to the GSLB ServerIron ADX every 7 seconds.

In order to change the health status interval for ServerIron ADX 1.1.1.108 to 4 seconds, configure the following on the ServerIron ADX 1.1.1.108.

```
SITE-ServerIronADX#conf t
SITE-ServerIronADX(config)#agent-health-report-interval 4
SITE-ServerIronADX(config)#end
```

ServerIron ADX 1.1.1.108 now starts sending health check status information to GSLB ServerIron ADX every 4 seconds. Note that this locally configured health status interval overrides the globally configured health status interval of 7 seconds.

Since the GSLB ServerIron ADX supports the distributed health check feature, the Flashback metric is disabled by default. Note that since site ServerIron ADX 1.1.1.108 supports the distributed health check, you should not enable the Flashback metric on the GSLB ServerIron ADX.

Example 2

In this example:

- The GSLB ServerIron ADX supports the distributed health check feature.
- Site ServerIron ADXs 1.1.1.105, ServerIron ADX 1.1.1.106 and ServerIron ADX 1.1.1.107 and ServerIron ADX 1.1.1.108 all belong to site “sunnyvale”.
- Only ServerIron ADX 1.1.1.105 supports the distributed health check feature. The other ServerIron ADXs do not support the distributed health check feature.

If most of the ServerIron ADXs at a site do not support the distributed health check feature and only a few ServerIron ADXs support the distributed health check feature, then the most concise way to configure this is to disable the distributed health check feature for the entire site and then individually enable it for the site ServerIron ADXs that support the distributed the health check feature.

In the above example, configure the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# conf t
GSLB-ServerIronADX(config)# gslb site sunnyvale
GSLB-ServerIronADX(config-gslb-site-sunnyvale)# no-distributed-health-check
GSLB-ServerIronADX(config-gslb-site-sunnyvale)#si 1.1.1.105
enable-si-dist-health-check
GSLB-ServerIronADX(config-gslb-site-sunnyvale)#e nd
```

Example 3

In this example:

- The GSLB ServerIron ADX does not support the distributed health check feature.
- Site ServerIron ADXs 1.1.1.105, ServerIron ADX 1.1.1.106 and ServerIron ADX 1.1.1.107 and ServerIron ADX 1.1.1.108 all belong to site “sunnyvale”.
- All the site ServerIron ADXs support the distributed health check feature.

The GSLB ServerIron ADX does not support the distributed health check feature, so the distributed health check configuration is neither supported nor applicable to the GSLB ServerIron ADX. The non-distributed health check GSLB ServerIron ADX and the distributed health check site ServerIron ADXs inter-operate without any special configuration; that is, no mandatory configuration is required to make them compatible.

Health check status interval configuration on the site ServerIron ADX does not apply to this topology. Flashback metric is enabled by default.

Example 4

In this example:

- The GSLB ServerIron ADX supports the distributed health check feature.
- Site ServerIron ADXs 1.1.1.105, ServerIron ADX 1.1.1.106 and ServerIron ADX 1.1.1.107 and ServerIron ADX 1.1.1.108 all belong to site “sunnyvale”.
- All the site ServerIron ADXs support the distributed health check feature.

If both the GSLB ServerIron ADX and the site ServerIron ADX support the distributed health check feature, then distributed health checking is enabled by default between them. In order to disable the distributed health check feature between distributed health check GSLB ServerIron ADX and distributed health check site ServerIron ADX, say ServerIron ADX 1.1.1.106, configure the following on the GSLB ServerIron ADX.

```
ServerIronADX(config)# gslb site sunnyvale
ServerIronADX(config-gslb-site-sunnyvale)# si-name 1.1.1.106
no-si-dist-health-check
ServerIronADX(config-gslb-site-sunnyvale)# end
```

This will disable distributed health check feature between GSLB ServerIron ADX and site ServerIron ADX 1.1.1.106 and now GSLB ServerIron ADX will carry out GSLB health checks for host servers being load balanced by site ServerIron ADX 1.1.1.106. Note that the distributed health check feature is still enabled between the GSLB ServerIron ADX and ServerIron ADXs 1.1.1.105, 1.1.1.107 and 1.1.1.108.

DNSSEC

DNSSEC (Domain Name System Security Extensions) is a set of extensions that provide DNS resolvers origin authentication of DNS data, data integrity and authenticated denial of existence. It protects DNS resolvers from forged DNS data (from cache poisoning, etc.). DNSSEC does not provide confidentiality.

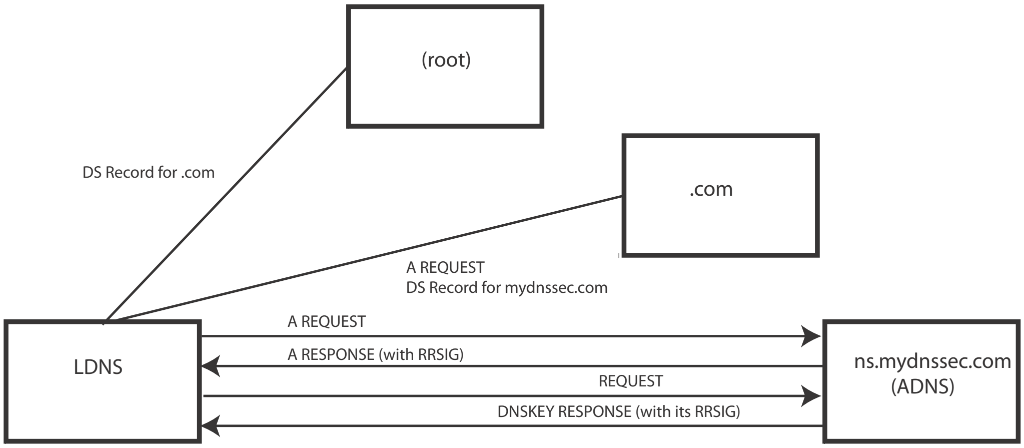
With DNSSEC, the responses are signed using public key cryptography. In addition to the answer RRsets, the response contains a RRSIG record which is an encrypted digital signature for the RRset. A DNSSEC aware client (resolver) sets the DO (DNSSEC OK) bit in the EDNS OPT section to indicate that it prefers DNSSEC signed responses. If the DO bit is set and if the server is DNSSEC capable, it copies the OPT section (including the DO bit) to the response and includes the DNSSEC signatures for each RRset in the response. The resolver can validate this signature by obtaining the public key of the ADNS server as a DNSKEY record.

Because the DO bit in EDNS is used to indicate DNSSEC responses and because the responses are in general larger due to the RRSIG records, a DNSSEC capable server (and the ServerIron ADX) must support EDNS and packet sizes of up to 4k. Also, if there are intermediate firewalls that drop fragmented UDP traffic, we'd have more resolvers retrying with TCP.

A DNSKEY record is validated via an "authentication chain". A well known public-key forms a "trust anchor" for this authentication chain. This can be used to verify a "designated signer" (DS) record—a signed hash of the DNSKEY of a child zone. Since the parent zone is trusted, the DS record validates the DNSKEY of the child zone. The child zone can contain other DS records to verify its child zones.

Signing KEYs are supposed to be changed regularly. However, for each new key, a child zone must have its parent zone create a DS record to validate the child zone's key. To simplify this, DNSSEC uses two keys—a zone-signing key (ZSK) and a key-signing key (KSK). All KEY records are signed with the KSK, and the entire zone is signed with the ZSK. The KSK is the key for which our parent publishes the DS record. The ZSK can be smaller and can be cycled more frequently (~monthly). The KSK is cycled less frequently (~annually). In such a scenario, a resolver would first validate the KSK through the parent zone DS record. A valid KSK is used to validate the RRSIG of the ZSK.

FIGURE 8 DNSSEC Example with Authentication Chain



The steps involved in a DNSSEC resolution are:

1. LDNS sends a normal type A request with the DO bit set to the mydnssec.com ADNS
2. If the ADNS supports DNSSEC, the response has the DO bit set and a RRSIG record for the response RRset in the answer section
3. The LDNS will then fetch the DNSKEY used in the RRSIG from the ADNS
4. DNSKEY validation at the LDNS occurs as follows:
   - It is configured to trust the DNSKEY for the root (.).
   - It fetches the DS record for the .com zone from the root.
   - It fetches the DNSKEY for the .com zone from the .com name server. This DNSKEY would be validated by checking against the signed hash in the DS record from the previous step.
   - It fetches the DS record for the mydnssec.com zone from the .com nameserver
   - This DS record validates the DNSKEY that was obtained from the mydnssec.com ADNS

Verification with DIG

The following example shows dig being used to validate a DNSSEC response.

```
[16:31:54 root@rhl-236 ~]# dig +dnssec mydnssec.com +multiline +sigchase
+trusted-key=/root/dnssec/Kmydnssec.com.+005+08340.key
;; RRset to chase:
mydnssec.com.           86400 IN A 10.35.62.235

;; RRSIG of the RRset to chase:
mydnssec.com.           86400 IN RRSIG A 5 2 86400 20100513221145 (
                                20100413221145 8340 mydnssec.com.
                                XdrNlVeH/Hc6sMCAOFCWerqtFRgCyNNlOcHrwnLZ+ApI
                                plN2t2QdpmEqhltmNyINJK2WH6xzP59bkynjOUcg8QQr
                                OBPRyjlZCXkTS0y8JFNGd0OIjW8KJkLmZ/cag0zFcvA+
                                xvNQsSM5w9hiprH364JDhSoQYASxFslLkX+MtGw= )

Launch a query to find a RRset of type DNSKEY for zone: mydnssec.com.

;; DNSKEYset that signs the RRset to chase:
mydnssec.com.           86400 IN DNSKEY 256 3 5 (
                                AwEAAacXnVRCUEnP7nRuCaGHWw5K7H+IedN5xWnnCUfe
                                f9upLZESWMPiY0b08biliRQ5Uqt6wCNINM9nBGGxxOhV
                                i/oT+DEkrjOhNN4o5L7Bd+PwYV0Vh+Fq383jvGdHtr8n
                                Q+mc69OgQjdARn6ofH6sDcOQFsvKsgtA/EQUa/mc9V2B
                                ) ; key id = 8340

;; RRSIG of the DNSKEYset that signs the RRset to chase:
mydnssec.com.           86400 IN RRSIG DNSKEY 5 2 86400 20100513221145 (
                                20100413221145 8340 mydnssec.com.
                                WdGTjFIGfFf6jpTm04iDYIj44WgvG+XMGJyzMS7jC5k7
                                LYk8HtjUAjVs920sgrz9HED7JKs9tMjzIiPZEKRsa+HI
                                7Re2Rvvrb5PbwNwWFi/smDI57NztLvCNoOWdYEk1r6jW
                                S8YVLnvd5rsN9d2DY+wr8UZSemRWAURn8G3GRLA= )

Launch a query to find a RRset of type DS for zone: mydnssec.com.
;; NO ANSWERS: no more

;; WARNING There is no DS for the zone: mydnssec.com.

;; WE HAVE MATERIAL, WE NOW DO VALIDATION ;; VERIFYING A RRset for mydnssec.com.
with DNSKEY:8340: success ;; OK We found DNSKEY (or more) to validate the RRset
;; Ok, find a Trusted Key in the DNSKEY RRset: 8340 ;; VERIFYING DNSKEY RRset for
mydnssec.com. with DNSKEY:8340: success

;; Ok this DNSKEY is a Trusted Key, DNSSEC validation is ok: SUCCESS

[16:32:06 root@rhl-236 ~]#
```

DNSSEC GSLB in DNS proxy mode

The ServerIron ADX supports GSLB for DNSSEC in the DNS proxy mode. In this mode, when the ServerIron ADX sees a DNS response, it re-orders the response such that it has the 'best IP address' as the first address in the answer RRset. It also sets the TTL of each of the answer records (This is for UDP). In the ADNS or the LDNS, the signature in the RRSIG record is calculated by ordering the individual resource records in canonical order. Only the RR type, class and the value

(IP address) are used in the signature. The TTLs of individual resource records are not part of the data used in signing to allow for aging. Since the TTL of the RRSIG record is part of the signed data, a caching resolver is expected to cache a response up to the minimum (smallest RR TTL in RRset, RRSIG record TTL).

With this approach a DNSSEC response can be performed without having to re-sign DNSSEC responses and without the need for key management.

With DNSSEC, due to the introduction of new record types, the size of a response can be much larger than plain DNS. EDNS0 with a buffer size of 4k is mandated by the RFC. Therefore we support UDP fragmented and TCP segmented DNS response.

The ServerIron ADX GSLB solution in the DNS proxy mode transparently acts upon DNS responses. If a ADNS real server or a zone is flagged for DNSSEC through configuration, it enables additional functionality such as accounting and real server selection. Zones can be tagged as DNSSEC ONLY or DNSSEC CAPABLE and real servers can be tagged as DNSSEC CAPABLE.

When some real servers are DNSSEC capable and some are not, all DNS requests are sent with the DO (DNSSEC OK) bit set to DNSSEC capable servers and other requests to the other servers.

When a zone is tagged as DNSSEC capable or DNSSEC only, requests to these zones are sent to DNSSEC capable real servers and requests to other zones are sent to other real servers. Through explicit configuration, plain DNS requests can be load balanced across all real servers.

If a zone is tagged as DNSSEC only, DNS requests are dropped.

Cache proxy mode

When cache proxy policy is configured with DNS proxy, the ServerIron ADX sends the response from its cache using the data learned from out-of-band backend DNS queries. However, for requests with the DO bit set if a real server is tagged as DNSSEC capable or if the zone is tagged for DNSSEC we forward the requests to the real server. If neither the zone or the server are tagged for DNSSEC, then we retain current behavior and respond directly.

Configuring DNSSEC for GSLB

The following sections describe how to configure a ServerIron ADX for DNSSEC.

Configuring a zone for DNSSEC

You can configure a zone to be DNSSEC capable or as DNSSEC only operation. as shown in the following:

```
ServerIron(config)# gslb dns zone-name brocade.com
ServerIron(config-gslb-dns-brocade.com)# dnssec-capable
```

Syntax: [no] dnssec-capable | dnssec-only

Configuring a backend ADNS server as DNNSEC capable

To configure a backend ADNS server as DNNSEC capable, use the following command.

```
ServerIron(config)# server real-name dns_ns 209.157.23.46
ServerIron(config-rs-dns_ns)# port dns proxy
ServerIron(config-rs-dns_ns)# port dns dnssec-capable
```

Syntax: dnssec-capable

Configuring load balancing of plain DNS request across all servers

If zones and real servers are configured for DNSSEC, then non-dnssec servers are used for requests on non-dnssec zones. To load-balance non-dnssec (plain DNS) requests across all servers, use one of the following commands.-

```
ServerIron(config)# server virtual dns_vip 209.157.23.46
ServerIron(config-vs-dns_vip)# port dns
ServerIron(config-vs-dns_vip)# port dns use-dnssec-servers-for-dns-queries
```

Syntax: [no] port dns use-dnssec-servers-for-dns-queries

```
ServerIron(config)# server use-dnssec-servers-for-dns-queries
```

Syntax: [no] server use-dnssec-servers-for-dns-queries

Displaying DNSSEC configuration

You can use the **show glsb zone** command to determine if a GSLB zone has be configured as dnssec-capable or dnssec-only. In the following example, the GSLB zone "secure.mydnssec.com" is configured as "DNSSEC-ONLY"

```
 ServerIronADX(config)# show gslb dns zone

 ZONE: secure.mydnssec.com
 HOST: null-host:
 (Global GSLB policy)
 GSLB affinity group: global
 DNSSEC-ONLY
                                              Flashback    DNS resp.
                                              delay        selection
                                              (x100us)     counters
                                              TCP  APP     Count (%)
 *   192.168.1.101: dns real-ip DOWN   N-AM     --   --    ---
 *   192.168.1.102: dns real-ip DOWN   N-AM     --   --    ---
 *  192.168.13.100: dns v-ip    ACTIVE N-AM      0    0    ---
 *   192.168.1.100: dns real-ip DOWN   N-AM     --   --    ---
```

Syntax: show gslb dns zone

Displaying DNSSEC statistics

When DNSSEC is enabled (by either real server or zone), DNSSEC statistics are displayed as shown in the following:

```
ServerIronADX# show gslb global-statistics

DNS proxy statistics:
TCP response         =          4 UDP response         =          5
Query type A         =          8 Query type ANY       =          1
DNSSEC response      =          3

DNS cache proxy stat:
Direct response      =          0

DNS query intercept stat:
Redirect             =          0  Direct response      =          0

Unsupported query types stat:
Error handling cnt   =          0
```

Syntax: show gslb global-statistics

Host-level policies for site selection

ServerIron ADX provides the following support for configuring GSLB policies for specified GSLB hosts:

- Configuring GSLB policies and apply them to hosts within GSLB domains
- Applying the global GSLB policy to all hosts
- Applying a host-level GSLB policy to one or more hosts
- Applying the global GSLB policy to some hosts and host-level GSLB policies to other hosts

Global vs host-level policy

The parameters for a host-level GSLB policy are similar to the parameters for the global GSLB policy. However, not all global GSLB parameters are available at the host level.

You can configure the following GSLB parameters under the global GSLB policy only:

- Geographic prefix (**geo-prefix** command) (see "Geographic region for a prefix" on page 129)
- Static prefix (**static-prefix** command)
- Health-status reporting interval (**health-status-interval** command)
- GSLB protocol update interval (**protocol status-interval** command)

Configuring host-level policies

Host-level GSLB policies provide finer granularity in specifying the GSLB metrics, related parameters, and the metric order, by applying them at the host level.

To configure a host-level GSLB policy, complete the following tasks.

1. Define a name for the host-level GSLB policy. Refer to page 118.
2. Configure the parameters for the policy. Refer to page 118.
3. Apply the policy to a host or multiple hosts. Refer to page 125.

Defining a name for a host-level GSLB policy

To define a name for a host-level GSLB policy, enter commands such as the following:

```
GSLB ServerIronADX# config t
GSLB ServerIronADX(config)# gslb-host-policy abc
GSLB ServerIronADX(config-gslb-host-policy-abc)#
```

The commands create a host-level GSLB policy named **abc**.

Syntax: [no] gslb-host-policy <*policy name*>

Configuring the parameters for the host-level policy

Enabling the active bindings metric

To enable the active bindings metric for a host-level GSLB policy, enter commands such as the following:

```
GSLB ServerIronADX(config)# gslb-host-policy abc
GSLB ServerIronADX(config-gslb-host-policy-abc)# active-bindings
```

Syntax: [no] active-bindings

Enabling the Capacity Threshold metric

You can enable the capacity threshold metric for a host-level GSLB policy. This metric represents a site ServerIron ADX’s available TCP/UDP session capacity. This metric is enabled by default, which means the GSLB ServerIron ADX uses this metric when evaluating the sites in a DNS reply to choose the best site.

To enable the capacity threshold metric, enter commands such as the following:

```
GSLB ServerIronADX(config)# gslb-host-policy abc
GSLB ServerIronADX(config-gslb-host-policy-abc)# capacity
```

Syntax: [no] capacity

Use the **no** form of the command to disable the Capacity Threshold metric.

NOTE
To configure a Capacity Threshold value, do so at the global GSLB policy level. The GSLB ServerIron ADX will apply this value to the host-level GSLB policy.

Enabling the connection load metric

To enable the Connection Load metric for a host-level GSLB policy, enter commands such as the following:

```
GSLB ServerIronADX(config)# gslb-host-policy abc
GSLB ServerIronADX(config-gslb-host-policy-abc)# connection-load limit 4
```

Syntax: [no] connection-load limit <*value*>

Use the **no** form of the command to disable the Connection Load metric.

You must specify a connection limit to enable the Connection Load metric. You can specify a value from 1 to as high a value as you need. There is no default. However, the actual value of the Connection Load limit, and other connection load parameters, will be obtained from the global GSLB policy.

Other connection load parameters include the following:

- Sampling intervals and sample rate
- Interval weights

NOTE
If the Connection Load limit is not configured in a host-level GSLB policy, but is configured in the global GSLB policy, and the host-level GSLB policy is applied to a host, the Connection Load metric will not be used during the GSLB selection process for that host/zone. The Connection Load limit configuration for the host-level GSLB policy serves as a way to enable or disable the Connection Load metric for a host when it is enabled in the global GSLB policy.

Removing IP addresses that fail a health check from DNS replies

You can configure the ServerIron ADX to remove IP addresses from DNS replies, for those hosts to which the host-level GSLB policy applies, when those addresses fail a health check. The ServerIron ADX removes the addresses that fail the check so long as the DNS query still contains at least one address that passes the health check.

A site must pass all applicable health checks (Layer 4 and Layer 7) to avoid being removed.

NOTE
If all the sites fail their health checks, resulting in all the sites being rejected by the GSLB ServerIron ADX, the ServerIron ADX sends the DNS reply unchanged to the client.

To configure the ServerIron ADX to remove IP addresses from DNS replies when those addresses fail a health check, enter commands such as the following:

```
ServerIronADX(config)# gslb host-policy abc
ServerIronADX(config-gslb-host-policy-abc)# dns active-only
```

Syntax: [no] dns active-only

Use the **no** form of the command to disable this DNS parameter.

Removing all IP addresses except the best address

By default, the GSLB ServerIron ADX retains the same number of IP addresses in the DNS replies from the DNS server. The GSLB policy swaps the IP address on the top of the list with the “best” address, selected by the GSLB policy.

You can configure the ServerIron ADX to remove all addresses except the one the host-level GSLB policy selects as the best address, by entering commands such as the following:

```
ServerIronADX(config)# gslb host-policy abc
ServerIronADX(config-gslb-host-policy-abc)# dns best-only
```

Syntax: [no] dns best-only

Use the **no** form of the command to disable this DNS parameter.

NOTE
If the GSLB policy does not result in the selection of a “best” address, the DNS reply can still contain multiple addresses.

Some of the DNS parameters are not configurable in the host-level GSLB policy. These parameters include:

- **dns cache-proxy**: Enables the ServerIron ADX to act as a proxy for a DNS server, by responding directly to the client queries without forwarding them to the DNS server
- **dns check-interval**: Changes the refresh interval for DNS queries to refresh verify zone and host information. The GSLB ServerIron ADX sends the queries to the DNS for which it is configured to be a proxy.
- **dns cname-detect:** Enables the ServerIron ADX to apply GSLB to CNAME records.
- **dns override**: Replaces the IP address in the DNS reply with the IP address you configure for the proxy server.
- **dns transparent-intercept**: Enables the DNS transparent intercept feature.
- **dns ttl:** Specifies the value to which the GSLB ServerIron ADX changes the TTL of each DNS record contained in DNS replies received from the DNS for which the ServerIron ADX is a proxy.

The GSLB ServerIron ADX will use these DNS parameters from the global GSLB policy for the host-level GSLB policy.

Disabling or re-enabling the Flashback metric

The Flashback metric indicates how quickly the GSLB ServerIron ADX receives Layer 4-7 health check results. This metric is enabled by default, which means the GSLB ServerIron ADX uses this metric when evaluating the sites in a DNS reply to choose the best site.

To disable this metric, enter the following command.

```
ServerIronADX(config)# gslb-host-policy abc
ServerIronADX(config-gslb-host-policy-abc)# no flashback
```

To re-enable this metric, enter the following command.

```
ServerIronADX(config)# gslb-host-policy abc
ServerIronADX(config-gslb-host-policy-abc)# flashback
```

Syntax: [no] flashback

NOTE
When both the Health Check metric and the Flashback metric are disabled for the host-level GSLB policy, the GSLB ServerIron ADX will not perform any Layer 4 or Layer 7 health checks for the hosts/zones to which this policy applies.

Modifying Flashback tolerance

You can modify the following Flashback parameters:

- Application tolerance
- TCP tolerance

The GSLB ServerIron ADX uses a tolerance value when comparing the Flashback speeds of different sites. The tolerance value specifies the percentage by which the Flashback speeds of the two sites must differ in order for the ServerIron ADX to choose one over the other. The default Flashback tolerance is 10%. Thus, if the Flashback speeds of two sites are within 10% of one another, the ServerIron ADX considers the sites to be equal. However, if the speeds differ by more than 10%, the ServerIron ADX prefers the site with the lower Flashback speed.

Flashback speeds are measured at Layer 4 for all TCP/UDP ports. For the application ports known to the ServerIron ADX, the Flashback speed of the application is also measured.

When the ServerIron ADX compares the Flashback speeds, it compares the Layer 7 (application-level) Flashback speeds first, if applicable. If the application has a Layer 7 health check and if the Flashback speeds are not equal, the ServerIron ADX is through comparing the Flashback speeds. However, if only the Layer 4 health check applies to the application, or if further tie-breaking is needed, the ServerIron ADX then compares the Layer 4 Flashback speeds.

To modify the application (Layer 7) tolerance, TCP (Layer 4) tolerance, or both, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# flashback application tolerance
30
GSLB-ServerIronADX(config-gslb-host-policy-abc)# flashback tcp tolerance 50
```

Syntax: **[no] flashback application | tcp tolerance** <*num*>

The **application | tcp** parameter specifies whether you are modifying the tolerance for the Layer 4 TCP health check or the Layer 7 application health checks. You can change one or both and the values do not need to be the same. For each, you can specify from 0-100. The default for each is 10.

Enabling the Geographic metric

The geographic metric indicates the geographic location of a site. This metric is enabled by default, which means the GSLB ServerIron ADX uses this metric when evaluating the sites in a DNS reply to choose the best site.

To enable the Geographic metric for a host-level GSLB policy, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# geographic
```

Syntax: **[no] geographic**

Use the [no] form of the command to disable the Geographic metric.

Enabling the Health Check metric

To enable the Health Check metric for the host-level GSLB policy, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# health-check
```

Syntax: **[no] health-check**

Use the [no] form of the command to disable the Health Check metric.

NOTE
When both the Health Check metric and the Flashback metric are disabled for a host-level GSLB policy, the GSLB ServerIron ADX will not perform any Layer 4 or Layer 7 health checks for the hosts/zones for which the policy applies.

Changing the order of the metrics

You can change the order in which the GSLB ServerIron ADX applies the policy metrics for the host-level policy. To change the order, specify the metrics in the desired order, such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# metric-order set health-check
round-trip-time capacity num-session flashback
```

Syntax: [no] metric-order set <*list*>

The <*list*> parameter is a list of the metrics you want to use, in the order you want the GSLB ServerIron ADX to use them for the host-level policy. The GSLB ServerIron ADX uses the metrics in the order you specify. You can specify one or more of the following:

- **active bindings**: The ServerIron ADX's preference for the IP address with the highest number of active bindings
- **capacity:** The remote ServerIron ADX's session capacity threshold.
- **connection-load:** The site ServerIron ADX's average number of new connections per second
- **flashback:** The site ServerIron ADX's Flashback speed (how quickly the GSLB receives the health check results)
- **geographic**: The geographic location of the server
- **health-check:** The Layer 4 and application health checks
- **num-session:** The remote ServerIron ADX's available session capacity
- **preference:** The administratively configured preference for the site ServerIron ADX
- **round-trip-time:** The round-trip time between the remote ServerIron ADX and the DNS client
- **weighted ip**: The administratively configured traffic distribution method for the ServerIron ADX based on weights for IP addresses
- **weighted site:** The administratively configured traffic distribution method for the ServerIron ADX based on weights for GSLB Sites

There are no parameters for the least response selection or round robin selection metrics. These metrics are tie-breakers. Only one of them is enabled at a time and the one that is enabled will always be the last metric in the host-level policy.

NOTE

We recommend that you always use the health check as the first metric. Otherwise, it is possible that the GSLB policy will not select a "best" choice, and thus send the DNS reply unchanged. For example, if the first metric is geographic location, and the DNS reply contains two sites, one in North America and the other in South America, for clients in South America the GSLB policy favors the South American site after the first comparison. However, if that site is down, the GSLB policy will find that none of the sites in the reply is the "best" one, and thus send the reply unchanged.

You cannot disable or change the position of the least response selection metric. The GSLB ServerIron ADX uses this metric as a tie-breaker if the other comparisons do not result is selection of a "best" site.

Resetting the order of the metrics

To reset the order of the GSLB policy metrics in a host-level policy to the default order, and re-enable all disabled metrics, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# metric-order default
```

Syntax: metric-order default

Enabling the Num-session metric

The capacity threshold specifies how close to the maximum session capacity the site ServerIronADX (remote ServerIron ADX) can be and still be eligible as the best site for the client. This mechanism provides a way to shift load away from a site before the site becomes congested. The GSLB ServerIron ADX uses this metric when evaluating the sites in a DNS reply to choose the best site.

To enable the num-session metric for a host-level policy, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# num-session
```

Syntax: [no] num-session

Use the **no** form of the command to disable the Num-session metric.

Configuring the Num-session Tolerance

You can specify the percentage by which the number of available sessions on the site ServerIron ADX can differ from the number of available sessions on another site ServerIron ADX and still be considered an equally good site. To do this, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# num-session tolerance 20
```

Syntax: [no] num-session tolerance *<num>*

The *<num>* parameter specifies the maximum percentage by which the session table utilization on ServerIron ADXs at different sites can differ without the GSLB ServerIron ADX selecting one over the other based on this metric. You can specify a tolerance from 0-100. The default is 10.

Enabling the Preference metric

To enable the Preference metric for a host-level policy, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# preference
```

Syntax: [no] preference

Use the **no** form of the command to disable the Preference metric.

Enabling the Round-Robin Selection metric

The round robin selection metric is an alternative to the least response selection metric as the final tie breaker. When you enable round robin selection, the GSLB ServerIron ADX automatically disables the least response selection metric, and instead uses the round robin algorithm for GSLB selection.

Use the round robin selection metric instead of the least response selection metric when you want to prevent the GSLB ServerIron ADX from favoring new or recently recovered sites over previously configured active sites.

The round robin selection metric is disabled by default. When you enable the metric, the software automatically disables the least response selection metric, since they are mutually exclusive. Likewise, if you disable the round robin selection metric, the software automatically re-enables the least response selection metric.

To enable round robin selection for a host-level policy, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# round-robin
```

Syntax: [no] round-robin

Enabling the Round-Trip-Time metric

You can enable the GSLB metric for the round-trip time between the remote ServerIron ADX and the DNS client.

The Round-trip time (RTT) is the amount of time that passes between when the remote site initiates a TCP connection (sends a TCP SYN) to the client and when the remote site receives the client's acknowledgment of the connection request (sends a TCP ACK). The GSLB ServerIron ADX learns the RTT information from the site ServerIron ADXs through the GSLB protocol and uses the information as a metric when comparing site IP addresses. The GSLB ServerIron ADX uses this metric when evaluating the sites in a DNS reply to choose the best site.

You can enable or disable the Round Trip Time (RTT) metric and configure RTT tolerance for the host-level policy. You can configure other parameters for the global GSLB policy, but not for the host-level policy. If a host-level policy is applied to a host/zone, then the GSLB ServerIron ADX will use the values defined in the global GSLB policy for RTT parameters that cannot be configured under the host-level policy. These parameters are:

- RTT cache interval
- RTT cache prefix length
- RTT explore percentage

To enable the Round Trip Time metric for the host-level policy, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# round-trip-time
```

Syntax: [no] round-trip-time

Changing the RTT tolerance

To change the RTT tolerance for the host-level policy, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# round-trip-time tolerance 20
```

Syntax: [no] round-trip-time tolerance <*num*>

Enabling the weighted IP metric

The weighted IP metric provides a way for the ServerIron ADX to distribute GSLB traffic among IP addresses in a DNS reply, based on weights assigned to the IP addresses.

To enable weighted IP for the host-level policy, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# weighted-ip
```

Syntax: [no] weighted-ip

Use the **no** form of the command to disable the weighted IP metric for the host-level policy.

Enabling the weighted site metric

The weighted site metric provides a way for the ServerIron ADX to distribute SLB traffic among GSLB sites based on weights configured for the sites.

To enable the weighted site metric for a host-level policy, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb-host-policy abc
GSLB-ServerIronADX(config-gslb-host-policy-abc)# weighted-site
```

Syntax: [no] weighted-site

Use the **no** form of the command to disable the weighted IP metric for the host-level policy.

Applying a host-level policy to a GSLB host

To apply a configured host-level policy to a GSLB host, enter commands such as the following:

```
GSLB-ServerIronADX(config)# gslb dns zone gslb1.com
GSLB-ServerIronADX(config-gslb-dns-gslb1.com)# host-info www http
GSLB-ServerIronADX(config-gslb-dns-gslb1.com)# host-info www gslb-policy abc
```

Syntax: **host-info** <*host*> **gslb-policy** <*policy-name*>

NOTE
By default, the GSLB ServerIron ADX applies the global GSLB policy to a host.

Displaying host-level policy information

Displaying a host-level policy

To view a particular host-level GSLB policy, enter a command such as the following:

```
GSLB-ServerIronADX# show gslb policy host-policy-name abc
GSLB POLICY: abc
  Default metric order: ENABLE
  Metric processing order:
                1-Server health check
                2-Remote ServerIron's session capacity threshold
                3-Round trip time between remote ServerIron and client
                4-Geographic location
                5-Site connection load
                6-Remote ServerIron's available session capacity
                7-VIP's active bindings
                8-Server flashback speed
                9-Remote ServerIron's preference value
                10-Local least response selection

  DNS active-only: ENABLE   DNS best-only: ENABLE
  Session availability tolerance: 20%
  Round trip time tolerance: 20
  Flashback appl-level delay tolerance: 30%, TCP-level delay tolerance: 50%
  Connection load limit: 4

  Weighted Site Metric: DISABLE     weighted IP Metric: DISABLE
  Active Bindings Metric: ENABLE
```

Syntax: **show gslb policy host-policy-name** <*policy-name*>

Displaying all GSLB policies

To view all defined host-level policies, enter the following command.

```
GSLB-ServerIronADX# show gslb policy host-policy-all

GSLB POLICY: abc
  Default metric order: ENABLE
  Metric processing order:
                1-Server health check
                2-Remote ServerIron's session capacity threshold
                3-Round trip time between remote ServerIron and client
                4-Geographic location
                5-Site connection load
                6-Remote ServerIron's available session capacity
                7-VIP's active bindings
                8-Server flashback speed
                9-Remote ServerIron's preference value
                10-Local least response selection

  DNS active-only: ENABLE   DNS best-only: ENABLE
  Session availability tolerance: 20%
  Round trip time tolerance: 20
  Flashback appl-level delay tolerance: 30%, TCP-level delay tolerance: 50%
  Connection load limit: 4

  Weighted Site Metric: DISABLE     Weighted IP Metric: DISABLE
  Active Bindings Metric: ENABLE

GSLB POLICY: test
  Default metric order: ENABLE
  Metric processing order:
                1-Remote ServerIron's session capacity threshold
                2-Round trip time between remote ServerIron and client
                3-Geographic location
                4-Remote ServerIron's available session capacity
                5-Least response selection


  DNS active-only: DISABLE  DNS best-only: DISABLE
  Session availability tolerance: 10%
  Round trip time tolerance: 10
  Connection load: DISABLE
  Weighted Site Metric: DISABLE     Weighted IP Metric: DISABLE
  Active Bindings Metric: DISABLE
```

Syntax: show gslb policy host-policy-all

Displaying the policy used for hosts

To view which GSLB policy is being used for hosts, enter the following command.

```
ServerIronADX# show gslb dns zone
ZONE: gslb1.com
HOST: www:
(GSLB policy: test)
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*       1.1.1.101: dns v-ip    ACTIVE N-AM      0    0    1 (100%)
*        1.1.1.22: dns real-ip ACTIVE N-AM     22   16    0 (0%)
*    10.10.10.200: dns real-ip DOWN   N-AM     --   --    0 (0%)
*        1.1.1.76: dns v-ip    DOWN   N-AM     --   --    0 (0%)


ZONE: gslb3.com
HOST: www:
(Global GSLB policy)
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*       1.1.1.102: dns v-ip    ACTIVE N-AM      0    0    1 (100%)
```

The output above shows that host policy “test” is in use for host “www” of zone “gslb1.com” and the global GSLB policy is in use for host “www” of zone “gslb3.com”.

Syntax: **show gslb dns zone I detail**

Displaying the number of host-level policies

To view the number of host-level policies configured and the maximum number of policies that can be configured, enter the following command.

```
GSLB-ServerIronADX# show gslb resources
GSLB resource usage:
                    Current   Maximum
sites               3         128
ServerIrons         1         256
ServerIrons' VIPs   2         2048
dns zones           1         256
dns hosts           1         1024
health-checks app.  1         1024
dns IP addrs.       4         2048
affinities          0         128
static prefixes     2         250
user geo prefixes   0         64
prefix cache        110       10128
RTT entries         0         20000
GSLB host policies  2         100
```

The “Current” column for GSLB host policies shows the number of host-level policies defined, and the “Maximum” column shows how many host-level policies can be configured in all. This example output shows that you can configure 98 more GSLB host policies.

Syntax: **show gslb resources**

Deleting GSLB host-level policies

Deleting a policy that is not applied to a host

You can delete a host-level GSLB policy directly using the **no gslb host-policy-name** <*policy-name*> command as long as the policy is not applied to a host. If the policy is bound to a host, the GSLB ServerIron ADX will not allow you to delete the policy.

To delete a host-level GSLB policy that is not applied to a host, use the command **no gslb host-policy-name** <*policy-name*> on the GSLB ServerIron ADX.

Deleting a Policy That Has Been Applied to Hosts

To remove references to, and delete a policy from all hosts to which the policy has been applied, enter the following command on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# clear gslb host-policy abc
```

Syntax: **clear gslb host-policy** <*policy-name*>

To remove references to hosts and delete all host-level GSLB policies, enter the following command on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# clear gslb host-policy
```

Syntax: **clear gslb host-policy**

Configuration example

The example configures a host-level GSLB policy. In this example, the GSLB ServerIron ADX is providing GSLB for the following three domains:

- *www.gslb1.com* (IP addresses: 1.1.1.101 (Active), 1.1.1.23 (Down), 1.1.1.54 (Down)}
- ftp.gslb1.com (IP addresses: 1.1.1.78 (Active), 1.1.1.76 (Down)}
- ftp.foo.com (IP addresses: 1.1.1.101 (Active), 1.1.1.23 (Active), 1.1.1.63 (Down)}

1. Define a host-level policy named "test" as follows.

```
GSLB-ServerIronADX(config)# gslb-host-policy test
GSLB-ServerIronADX(config-gslb-host-policy-test)# dns active-only
GSLB-ServerIronADX(config-gslb-host-policy-test)# metric-order set
health-check
GSLB-ServerIronADX(config-gslb-host-policy-test)# end
```

2. Configure the metric order for the GSLB policy.

```
GSLB-ServerIronADX# con t
GSLB-ServerIronADX(config)# gslb policy
GSLB-ServerIronADX(config-gslb-policy)# metric-order set health-check
GSLB-ServerIronADX(config-gslb-policy)# end
```

3. Apply the host-level policy to host “www” for zone gslb1.com and host “ftp” for zone foo.com.

```
GSLB-ServerIronADX#con t
GSLB-ServerIronADX(config)# gslb dns zone gslb1.com
GSLB-ServerIronADX(config-gslb-dns-gslb1.com)# host-info www http
GSLB-ServerIronADX(config-gslb-dns-gslb1.com)# host-info www gslb-policy test
```

```
GSLB-ServerIronADX(config-gslb-dns-gslb1.com)# exit
GSLB-ServerIronADX(config)# gslb dns zone foo.com
GSLB-ServerIronADX(config-gslb-dns-foo.com)# host-info ftp ftp
GSLB-ServerIronADX(config-gslb-dns-foo.com)# host-info ftp gslb-policy test
```

In the above example, with host policy “test” applied to host “www” for gslb1.com, when the ServerIron ADX receives client queries for *www.gslb1.com*, the GSLB ServerIron ADX returns only the healthy IP addresses with the best IP address at the top of the list (i.e., 1.1.1.101 only).

Since the global GSLB policy is in effect for host "ftp" for gslb1.com, when the ServerIron ADX receives client queries for ftp.gslb1.com, the GSLB ServerIron ADX will return all IP addresses for this domain with the best IP address at the top of the list (i.e., it returns 1.1.1.78 and 1.1.1.76).

Geographic region for a prefix

Brocade ServerIron ADX GSLB policies use a number of metrics, including the geographic location of a server, to evaluate the server IP addresses in a DNS reply.

The GSLB ServerIron ADX uses the Internet Assigned Numbers Authority’s (IANA’s) IP address prefixes (IPv4 or IPv6) to generate an initial static database of geographic prefixes. This database consists of IP address prefixes (IP address/prefix length) and their corresponding geographic locations, such as, the continent for each IP address prefix.

You can configure the geographic locations for an IP address prefix, or override an existing geographic region for an IP address prefix by configuring a new one. You can assign one of the following geographic locations to an IP address prefix:

- North America
- South America
- Europe
- Asia
- Africa

How geographic location is determined

Once you configure a geographic region for an IP address prefix, the GSLB ServerIron ADX determines the geographic region of a server in the following ways:

- For a real IPv4 or IPv6 address, the geographic region is based on the IP address. If you configure a geographic prefix that matches the real server IP address, the device obtains the geographic location of the real server from the geographic prefix entry that you configure.
- For a virtual IP address— a logical IP address configured on a site ServerIron ADX, the geographic region is based on the management IP address of the site ServerIron ADX on which the VIP is configured. If you configure a geographic prefix that matches the management IP address of the site ServerIron ADX on which the VIP is configured, the device obtains the geographic location of the VIP from the geographic prefix entry that you configure.
- If the management IP address of the remote ServerIron ADX at that site is not indicative of the geographic location, use the geo-location command to specify the region of the GSLB site. For more information about this command, see “Specifying site locations” on page 20.
  For example, if the management IP address is in a private subnet, the address is not indicative of the ServerIron ADX’s geographic location. If you specify the region for the GSLB site, the GSLB ServerIron ADX uses the region you specify instead of the region of the ServerIron ADX’s

management IP address.
If you configure a geographic prefix entry that matches the management IP address of the remote ServerIron ADX and also specify a geographic location for the GSLB site where the remote ServerIron ADX resides, then the geographic location configured for the GSLB site takes precedence over the one defined in the user-configured geographic prefix entry. For example, the geographic region for a VIP configured on the remote ServerIron ADX will be obtained from the geographic location configured for the GSLB Site where the remote ServerIron ADX resides instead of the geographic prefix entry that matches the management IP address of the remote ServerIron ADX.

The GSLB ServerIron ADX determines the geographic location of the client as follows: For each client query, the GSLB ServerIron ADX determines the geographic location from which the client query came based on its IP address.

- If the IP address prefix of a user-configured geographic prefix entry matches that of the client, then the geographic location of the client will be as specified in the user-configured geographic prefix entry.
- If multiple server IP addresses compare equally based on the GSLB metrics above the geographic metric in the GSLB policy, then the GSLB ServerIron ADX prefers server IP addresses within the same geographic region as the client query.

Configuring a geographic prefix

Using the **geo-prefix** command, you can configure the geographic location of an IP address prefix, or override an existing geographic region for an IP address prefix by configuring a new one.

You can assign one of the following geographic locations to an IP address prefix:

- North America
- South America
- Europe
- Asia
- Africa

For IPv4:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb policy
GSLB-ServerIronADX(config-gslb-policy)# geo-prefix 24.192.0.0/24 europe
GSLB-ServerIronADX(config-gslb-policy)# end
```

These commands create a geographic prefix entry with IPv4 address 24.192.0.0, prefix length 24, and geographic region Europe

For IPv6:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb policy
GSLB-ServerIronADX(config-gslb-policy)# geo-prefix 2001.db8::/64 asia
GSLB-ServerIronADX(config-gslb-policy)# end
```

These commands create a geographic prefix entry with IPv6 address 2001.db8::, prefix length 64, and geographic region Asia.

Syntax: [no] geo-prefix { *<ipv4-prefix>* | *<ipv6-prefix>*} [asia | europe | n-america | s-america | africa]

The command configures an association between a prefix and a geographic location. The *<ipv4-prefix>* and *<ipv6-prefix>* variables identify the respective networks. Five operands serve as location tags for the network: **asia**, **europe**, **n-america**, **s-america**, and **africa**.

NOTE
When a geographic prefix is converted from static to dynamic through geographic prefix configuration, the old geographic prefix information will be replaced with the new information. If the prefix is deleted, the old value will not be restored because it has already been replaced.

Displaying the number of geographic prefixes

To view the number of geographic prefixes defined on a GSLB ServerIron ADX, enter the following command.

```
GSLB-ServerIronADX# show gslb resources
GSLB resource usage:
                  Current   Maximum
sites               2         128
ServerIronADXs         0         256
ServerIronADXs' VIPs   0         2048
dns zones           1         256
dns hosts           1         1024
health-checks app.  1         1024
dns IP addrs.       0         2048
affinities          0         128
static prefixes     0         250
user geo prefixes   1         64
prefix cache        109       10128
RTT entries         0         20000
GSLB host policies  0         100
```

The “Current” column for user **geo prefixes** specifies the number of user-configured geographic prefixes. The "Maximum” column denotes the maximum number of geographic prefixes that you can configure. In the example above, there is one configured geographic prefix, and a maximum of 64 configurable geographic prefixes can be specified on the GSLB ServerIron ADX.

Syntax: show gslb resources

Displaying information about geographic prefix

To view information about a specific geographic prefix, enter the following command on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# show gslb cache 24.192.0.0
prefix length = 24, prefix = 24.192.0.0, region = EUROPE
prefix source = geographic (user-configured)
```

The output above shows the IP address prefix, prefix length, the geographic region and source (in this case it is a user-configured geographic prefix entry. For more examples, refer to “Displaying RTT information” on page 178.

Syntax: show gslb cache *<IP address prefix>*

To view all geographic prefixes on the GSLB ServerIron ADX, enter the following command.

```
GSLB-ServerIronADX# show gslb cache all geographic user-configured
prefix length = 24, prefix = 1.1.1.0, region = EUROPE
prefix source = geographic (user-configured),
prefix length = 24, prefix = 10.10.10.0, region = ASIA
prefix source = geographic (user-configured)
```

The output above shows the IP address prefix, prefix length, the geographic region and source (user-configured). For more examples, refer to "Displaying RTT information" on page 178.

Syntax: **show gslb cache all geographic user-configured**

Example configuration

In the following example, the GSLB ServerIron ADX provides GSLB for the domain *www.gslb1.com*.

1. Display the IP addresses for the domain *www.gslb1.com*, by entering the following command.

```
ServerIronADX# show gslb dns detail
ZONE: gslb1.com
HOST: www:
(Global GSLB policy)
                                             Flashback    DNS resp.
d                                            elay        selection
                                             (x100us)    counters
                                              TCP  App   Count (%
*        1.1.1.22: dns real-ip ACTIVE N-AM      5   16    ---
*    10.10.10.200: dns real-ip DOWN   N-AM     --   --    ---
*        1.1.1.76: dns v-ip    DOWN   N-AM     --   --    ---
                  site: local, weight:   0, ServerIronADX: 1.1.1.102
                  session util:   0%, avail. sessions: 5999976
                  preference: 128
*       1.1.1.101: dns v-ip    ACTIVE N-AM      0    0    ---
                  Active Bindings: 1
                  site: local, weight:   0, ServerIronADX: 1.1.1.102
                  session util:   0%, avail. sessions: 5999976
                  preference: 128
```

   As shown in the output, the current geographic location for all the IP addresses in the domain *www.gslb1.com* is North America (N-AM).

2. Configure the geographic prefix 1.1.1.42/24 and designate Asia as the geographic location.

```
ServerIronADX# con t
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# geo-prefix 1.1.1.42/24 asia
ServerIronADX(config-gslb-policy)# end
```

3. To display the contents of the entry, enter the **show gslb cache** command.

```
ServerIronADX# show gslb cache 1.1.1.42
prefix length = 24, prefix = 1.1.1.0, region = ASIA
prefix source = geographic (user-configured),
```

4. After you configure a geographic location for the prefix, the GSLB ServerIron ADX updates the geographic location for the IP addresses as explained in the section "How geographic location is determined" on page 129.

5. To view the geographic location of the IP addresses, enter the **show gslb dns detail** command.

```
ServerIronADX# show gslb dns detail

ZONE: gslb1.com
HOST: www:
(Global GSLB policy)
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*        1.1.1.22: dns real-ip ACTIVE ASIA      5   16    ---
*    10.10.10.200: dns real-ip DOWN   N-AM     --   --    ---
*        1.1.1.76: dns v-ip    DOWN   ASIA     --   --    ---
                  site: local, weight:   0, ServerIronADX: 1.1.1.102
                  session util:   0%, avail. sessions: 5999976
                  preference: 128
*       1.1.1.101: dns v-ip    ACTIVE ASIA      0    0    ---
                  Active Bindings: 1
                  site: local, weight:   0, ServerIronADX: 1.1.1.102
                  session util:   0%, avail. sessions: 5999976
                  preference: 128
```

The above output shows that the geographic location is Asia. The geographic location for 10.10.10.200 is still North America (N-AM) because it does not match the user-configured geographic prefix.

Smoothing mechanism for RTT measurements

A GSLB ServerIron ADX learns the Round Trip Time (RTT) information from the Site ServerIron ADXs through the GSLB protocol and uses the information as a metric when comparing IP addresses. For each RTT value reported by the Site ServerIron ADX, the GSLB ServerIron ADX calculates the effective RTT value by adding 90% of the existing RTT value in the cache entry to 10% of the new RTT sample to obtain the effective RTT value for that cache entry.

For example, assume Site ServerIron ADX 1.1.1.101 is periodically reporting the RTT for a client IP 1.1.1.42 to the GSLB. The first value that the Site ServerIron ADX reports to the GSLB ServerIron ADX is 20ms. The GSLB ServerIron ADX stores this RTT in its cache (1.1.1.101, rtt = 20ms). When the Site ServerIron ADX again reports RTT for 1.1.1.42, the GSLB ServerIron ADX uses the following formula to calculate the new RTT value.

effective RTT = 90 % of old RTT value + 10% of new RTT value

If the Site ServerIron ADX reports an RTT value of 40ms for 1.1.1.101, then effective RTT would be

90% of 20ms + 10% of 40ms = 22ms

This smoothing mechanism may not be effective in dealing with large variances in RTT measurements. For example, if the Site ServerIron ADX reports just one very high value, for example 1 second, then the RTT will be.

90% of 22ms + 10% of 1 sec = 119ms

After this calculation, even if the Site ServerIron ADX continues to report 20ms, it will take some time for the resulting RTT to come down to 20ms. This formula is not adaptive enough to deal with transient spikes in RTT values.

This release introduces a new smoothing mechanism along with a proprietary smoothing algorithm for GSLB RTT measurements to effectively deal with variances in RTT measurements. These mechanisms allow you to define what is a very high or a very low value for an RTT sample on the GSLB ServerIron ADX. If the new sample is in the acceptable range, GSLB ServerIron ADX will do a smoothing similar to the one described above. If the value is much higher than current RTT value, then GSLB ServerIron ADX will ignore this value a few times. If GSLB ServerIron ADX still sees this large value after ignoring it for some time, then it will factor this value into existing RTT using an additive increase. Similarly, if the value is much lower than current RTT, GSLB ServerIron ADX will ignore it a few times. If GSLB ServerIron ADX still sees this small value after ignoring it for sometime, then it will factor this value into the existing RTT value using a multiplicative decrease.

In the scenario described above, you can, for example, specify that anything more than 50% of the existing value should be considered a very high RTT and should be ignored once. If RTT was 20ms and the Site ServerIron ADX reported a new RTT of 1 second, then the GSLB ServerIron ADX will ignore this value once. If Site ServerIron ADX continues to report an RTT of 1 second, then this will be slowly factored into existing RTT value, using an additive increase.

Configuring enhanced RTT smoothing

To configure Enhanced RTT Smoothing, complete the following tasks.

1. Enable Enhanced RTT Smoothing. Refer to page 135.
2. Configure the parameters. Refer to page 136.

Parameters to smooth RTT variances

You can configure or modify the following parameters to customize enhanced RTT smoothing for your network:

- Maximum deviation allowed: This parameter defines the maximum acceptable deviation for an RTT sample. It defines what the GSLB ServerIron ADX should consider as a very high or a very low RTT value.

  For example, you may observe that the deviation between the old and new RTT value during a spike in the RTT is typically 500% of the existing RTT value. You can use this information to determine the optimal value for maximum deviation allowed. You can fine tune the value of maximum deviation allowed which in turn will determine which RTT samples should be considered as very high or very low as compared to the current RTT. The default value for this parameter will be 400%.

- Maximum ignore count: This counter defines how many consecutive very high or very low new RTT samples to ignore before factoring them into the existing RTT value.

  This count specifies how many extremely high or extremely low RTT values to ignore. The default is 3. If a spike in the RTT occurs once in a while, set this parameter to 1. If you do not want to ignore any samples, set this parameter to 0.

- Normal ramp factor: This parameter defines the factor by which a RTT sample in the acceptable range should be factored into the existing RTT value. This is typically around 10%.
- Ramp up factor: This parameter specifies the increments in which successively new high RTT samples should be factored into the existing RTT value.

Each successively high RTT sample will be gradually factored into the existing RTT value using an additive increase. The ramp up factor specifies the step for the additive increase. For example, if the ramp up factor is 2 and the normal ramp factor is 10, then the percent usage of the new RTT sample will increase in increments of 2 until it reaches 10, as follows: 1,3,5,7, 9,10. Note that the upper boundary (10 in this example) is determined by the normal ramp factor.

If you set a high value for maximum ignore count, then you may want the RTT value to ramp up quickly because the GSLB ServerIron ADX has already ignored enough RTT samples with high values. If GSLB ServerIron ADX is still seeing high values, this means they are not anomalies. In reality the RTT has increased and GSLB ServerIron ADX needs to factor this increased RTT into the existing RTT value quickly. You can set the ramp up factor to a higher value in order to achieve this.

NOTE
You may need to fine-tune both ramp up factor and the normal ramp factor if a faster ramp up in the RTT value is desired

- **Ramp down factor:** This parameter specifies the factor by which successively new very low RTT samples should be factored into the existing RTT value.

  Each successively low RTT sample will be factored into the existing RTT value using a multiplicative decrease. The ramp up factor specifies the step for the multiplicative decrease. For example, if ramp down factor is 3 and normal ramp factor is 10, then the percent usage of the new RTT sample will be in multiples of 3 until it reaches 10, as follows: 1,3,9,10. Note that the upper boundary is determined by the normal ramp factor.

  Again as described earlier, if you had set a high value for maximum ignore count, then you may want the RTT value to ramp down quickly. You can set the ramp down factor to a higher value in order to achieve this.

NOTE
You may need to fine-tune both ramp down factor and the normal ramp factor if a faster ramp down in the RTT value is desired

Enabling enhanced RTT smoothing

Enhanced RTT smoothing is disabled globally by default. You can enable enhanced RTT smoothing globally or per GSLB site.

Once enhanced RTT smoothing is enabled, you can configure the parameters for the feature. These parameters are configured for each site at the Site-level. This means that each site can have its own set of enhanced RTT smoothing parameters.

To enable enhanced RTT smoothing globally for all GSLB Sites, enter commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb enhanced-rtt-smoothing
```

Syntax: gslb enhanced-rtt-smoothing

To enable enhanced RTT smoothing for a GSLB Site, enter commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb site sanjose
GSLB-ServerIronADX(config-gslb-site-sanjose)# enable-site-rtt-smoothing
```

Syntax: enable-site-rtt-smoothing

Disabling enhanced RTT smoothing

To disable enhanced RTT smoothing for a GSLB Site, enter commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb site sanjose
GSLB-ServerIronADX(config-gslb-site-sanjose)#  disable-site-rtt-smoothing
```

Syntax: disable-site-rtt-smoothing

This command disables enhanced RTT smoothing for the specified site. If the feature is enabled globally, you can disable it for a particular site using this command.

Configuring the parameters

Specifying the maximum RTT deviation

If you want to specify the maximum RTT deviation allowed for a site, enter commands such as the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb site sanjose
GSLB-ServerIronADX(config-gslb-site-sanjose)# max-rtt-dev-allowed 300
```

Syntax: [no] max-rtt-dev-allowed <*percent*>

Enter a value from 50-100000 for <*percent*>. The default is 400 percent.

Specifying the maximum ignore count

The maximum ignore counter defines how many consecutive very high or very low new RTT samples to ignore before factoring them into the existing RTT value. If you want to specify the **`max-ignore-count`**, enter commands such as the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb site sanjose
GSLB-ServerIronADX(config-gslb-site-sanjose)# max-ignore-count 6
```

Syntax: [no] max-ignore-count <*value*>

Enter a number from 1-20 for <*value*>. The default is 3.

Specifying the normal ramp factor

The normal ramp factor defines the factor by which a RTT sample in the acceptable range should be factored into the existing RTT value. If you want to specify the normal ramp factor, enter commands such as the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb site sanjose
GSLB-ServerIronADX(config-gslb-site-sanjose)# normal-ramp-factor 20
```

Syntax: [no] normal-ramp-factor <*percent*>

Enter a value of 1-50 for percent>. The default is 10 percent.

Specifying the ramp-up-factor

The ramp-up factor specifies the increments in which successively new high RTT samples should be factored into the existing RTT value. If you want to specify the ramp-up factor, enter commands such as the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb site sanjose
GSLB-ServerIronADX(config-gslb-site-sanjose)# ramp-up-factor 4
```

Syntax: [no] ramp-up-factor <*value*>

Enter a number from 1-10 for <*value*>. The default is 2.

Specifying the ramp-down factor

The ramp-down factor specifies the factor by which successively new very low RTT samples should be factored into the existing RTT value. If you want to specify the ramp-down factor, enter the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb site sanjose
GSLB-ServerIronADX(config-gslb-site-sanjose)# ramp-down-factor 4
```

Syntax: [no] ramp-down-factor <*value*>

Enter a number from 1-10 for <*value*>. The default is 3.

Simulating RTT smoothing

You can test an enhanced RTT smoothing configuration for a Site ServerIron ADX before it is deployed by running the RTT smoothing simulator. This simulator is a tool that allows you to apply the new RTT smoothing mechanism for a GSLB Site on a set of sample RTT values. This simulator aids in determining the optimal values of enhanced RTT smoothing parameters such maximum deviation allowed, maximum ignore count, normal ramp factor, ramp up factor and ramp down factor. You can also use the simulator as a debugging tool to determine how a particular RTT value was derived. You can also compare the new and existing RTT smoothing mechanism results using this simulator and determine which of the two mechanisms is more suitable for your network.

Before using the simulator, you may first configure the desired enhanced RTT smoothing parameters (maximum deviation allowed, maximum ignore count, normal ramp factor, ramp up factor, and ramp down factor) for the GSLB Site. If you do not configure any enhanced RTT smoothing parameters for the Site, then the default values for the parameters are used during simulation.

To start the simulation for a GSLB Site, enter the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb simulate-rtt-smoothing test 5
GSLB-ServerIronADX(config-gslb-rtt-sim-test)#
```

Syntax: gslb simulate-rtt-smoothing <*site-name*> <*initial-rtt-value*>

Enter the name of the GSLB site for <*site-name*>.

Enter <*initial-rtt-value*>Initial RTT value

After enabling the simulator, the GSLB enters the enhanced RTT simulation mode for the GSLB Site specified. Also, by default, the enhanced smoothing mechanism is disabled during simulation. To enable the enhanced smoothing mechanism for simulation, enter the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# enable-sim-new-rtt-smooth
```

Syntax: **enable-sim-new-rtt-smooth**

This command enables enhanced RTT smoothing only for simulation purposes.

To disable the enhanced smoothing mechanism during simulation, configure the following:

```
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# disable-sim-new-rtt-smooth
```

Syntax: **disable-sim-new-rtt-smooth**

This command disables enhanced RTT smoothing only for simulation purposes.

You can now input the RTT values and the simulator will display the result of RTT smoothing of the RTT value. To input an RTT value, enter the following command.

```
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 6
```

Syntax: **rtt-val** <*value*>

Enter the new RTT sample value for <*value*>

To end the simulator, enter the exit command.

```
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# exit
```

Note that each time you exit the simulation submode, the simulation state gets cleared. You can clear the simulation state by entering the **gslb simulate-rtt-smoothing** command in the simulation mode.

Example

In the following example the simulator simulates the old (existing) RTT smoothing mechanism for a set of RTT samples.

```
GSLB-ServerIronADX(config)# gslb simulate-rtt-smoothing test 30
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 1
SIMULATOR: Enhanced RTT smoothing is OFF
RTT state before application of RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 30, RTT decimal val = 0.0
Applied RTT smoothing algorithm for new RTT sample 1
RTT state after application of RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 27, RTT decimal val = 0.0
GSLB-ServerIronADX(config-gslb-rtt-sim-test)#rtt-val 1000
SIMULATOR: Enhanced RTT smoothing is OFF
RTT state before application of RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 27, RTT decimal val = 0.0
Applied RTT smoothing algorithm for new RTT sample 1000
RTT state after application of RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 124, RTT decimal val = 0.0
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 30
SIMULATOR: Enhanced RTT smoothing is OFF
RTT state before application of RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 124, RTT decimal val = 0.0
Applied RTT smoothing algorithm for new RTT sample 30
RTT state after application of RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 114, RTT decimal val = 0.0
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 30
SIMULATOR: Enhanced RTT smoothing is OFF
```

```
RTT state before application of RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 114, RTT decimal val = 0.0
Applied RTT smoothing algorithm for new RTT sample 30
RTT state after application of RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 105, RTT decimal val = 0.0
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 30
SIMULATOR: Enhanced RTT smoothing is OFF
RTT state before application of RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 105, RTT decimal val = 0.0
Applied RTT smoothing algorithm for new RTT sample 30
RTT state after application of RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 97, RTT decimal val = 0.0
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 30
SIMULATOR: Enhanced RTT smoothing is OFF
RTT state before application of RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 97, RTT decimal val = 0.0
Applied RTT smoothing algorithm for new RTT sample 30
RTT state after application of RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 90, RTT decimal val = 0.0
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# exit
```

Example

The following example simulates the enhanced RTT smoothing mechanism for the same set of RTT samples used above; however, since parameters for the feature have not been configured for the Site "test", default values of the parameters are used.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb simulate-rtt-smoothing test 30
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# enable-sim-new-rtt-smooth
GSLB-ServerIronADX(config-gslb-rtt-sim-test)#rtt-val 1
SIMULATOR: Enhanced RTT smoothing is ON
RTT sample value 1 is acceptable
RTT state before application of enhanced RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 30, RTT decimal val = 0.0
 ignore-larger-rtt-count = 0
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
Applied enhanced RTT smoothing algorithm for new RTT sample 1
RTT state after application of enhanced RTT smoothing mechanism:
----------------------------------------------------------------
RTT value after smoothing = 27, RTT decimal val = 0.100
ignore-larger-rtt-count = 0
ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
GSLB-ServerIronADX(config-gslb-rtt-sim-test)#rtt-val 1000
SIMULATOR: Enhanced RTT smoothing is ON
RTT sample value 1000 is not acceptable (higher)
RTT state before application of enhanced RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 27, RTT decimal val = 0.100
 ignore-larger-rtt-count = 0
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
Applied enhanced RTT smoothing algorithm for new RTT sample 1000
RTT state after application of enhanced RTT smoothing mechanism:
```

```
----------------------------------------------------------------
 RTT value after smoothing = 27, RTT decimal val = 0.100
 ignore-larger-rtt-count = 1
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 30
SIMULATOR: Enhanced RTT smoothing is ON
RTT sample value 30 is acceptable
RTT state before application of enhanced RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 27, RTT decimal val = 0.100
 ignore-larger-rtt-count = 1
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
Applied enhanced RTT smoothing algorithm for new RTT sample 30
RTT state after application of enhanced RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 27, RTT decimal val = 0.390
 ignore-larger-rtt-count = 0
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 30
SIMULATOR: Enhanced RTT smoothing is ON
RTT sample value 30 is acceptable
RTT state before application of enhanced RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 27, RTT decimal val = 0.390
 ignore-larger-rtt-count = 0
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
Applied enhanced RTT smoothing algorithm for new RTT sample 30
RTT state after application of enhanced RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 27, RTT decimal val = 0.651
 ignore-larger-rtt-count = 0
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 30
SIMULATOR: Enhanced RTT smoothing is ON
RTT sample value 30 is acceptable
RTT state before application of enhanced RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 27, RTT decimal val = 0.651
 ignore-larger-rtt-count = 0
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
Applied enhanced RTT smoothing algorithm for new RTT sample 30
RTT state after application of enhanced RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 27, RTT decimal val = 0.885
 ignore-larger-rtt-count = 0
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# rtt-val 30
SIMULATOR: Enhanced RTT smoothing is ON
RTT sample value 30 is acceptable
RTT state before application of enhanced RTT smoothing mechanism:
------------------------------------------------------------------
 RTT val = 27, RTT decimal val = 0.885
 ignore-larger-rtt-count = 0
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
Applied enhanced RTT smoothing algorithm for new RTT sample 30
RTT state after application of enhanced RTT smoothing mechanism:
----------------------------------------------------------------
 RTT value after smoothing = 28, RTT decimal val = 0.96
 ignore-larger-rtt-count = 0
 ignore-smaller-rtt-count = 0, increment-rtt-factor = 1
```

```
GSLB-ServerIronADX(config-gslb-rtt-sim-test)# exit
```

Note that the resulting RTT value obtained after smoothing the following set of RTT samples (30,1,1000,30,30,30,30) using the old smoothing mechanism is 90.0. The result and is 28.96 with the enhanced smoothing mechanism.

Determining if the new RTT smoothing mechanism is enabled

To determine if the new RTT smoothing mechanism is enabled or disabled for a GSLB Site, enter the following command.

```
GSLB-ServerIronADX# show gslb site local
SITE: local
 Enhanced RTT smoothing: ON
ServerIron:  1.1.1.102:
state: SELF
Protocol Version: 2
distributed health-chk
 Current num.  Session   CPU load  Preference  Location  Connection
 sessions      util(%)   (%)       (0-255)               Load-Avg
     24        0          2         128        EUROPE         0
 Virtual IPs:

 1.1.1.101(A)         1.1.1.76(A)
```

Syntax: **show gslb site** <*site-name*>

The output above shows that the new RTT smoothing mechanism is enabled for GSLB Site "local".

Round-trip times

Brocade GSLB supports both passive and active round-trip time (RTT) gathering to determine the round-trip times between a Site ServerIron ADX and a client.

Passive RTT gathering

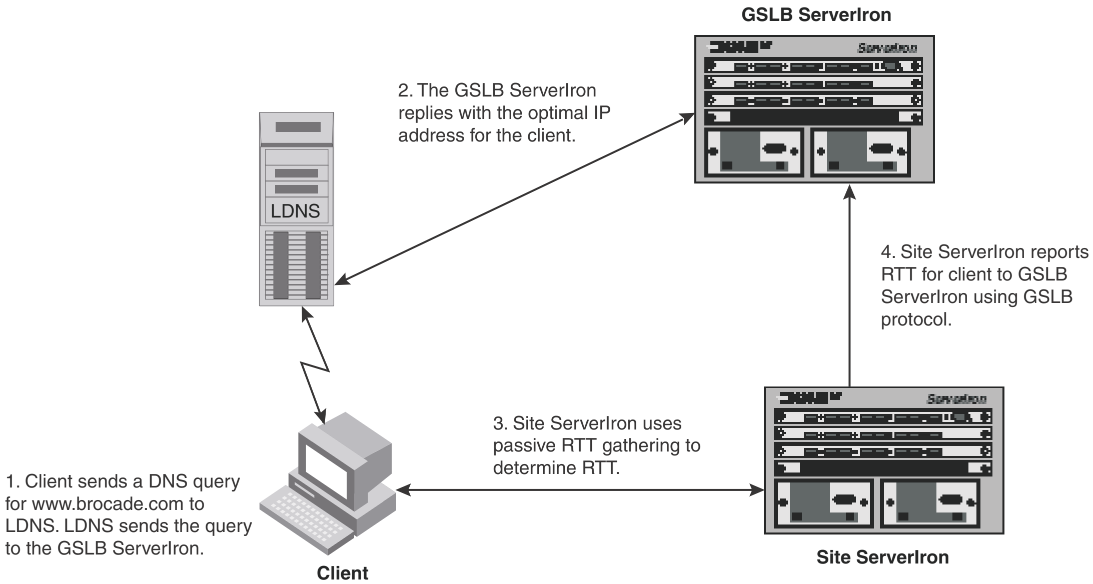
Passive RTT gathering uses the existing flow of traffic between the client and the Site ServerIron ADX to gather RTT. Whenever a client opens a TCP connection with the Site ServerIron ADX, the Site ServerIron ADX computes the round-trip time (RTT) as the amount of time that passes between the time the Site ServerIron ADX receives the TCP connection (TCP SYN) from the client, and when it receives the client's acknowledgment of the connection request (TCP ACK).

The Site ServerIron ADX uses the GSLB protocol to report the RTT to the GSLB ServerIron ADX. The GSLB ServerIron ADX uses this RTT information as a metric when comparing IP addresses in the DNS reply to select the optimal IP address for the client.

NOTE
Passive RTT information is not gathered on the remote site ServerIron ADX if the ServerIron ADX only processes basic load balance traffic and the **server no-fast-stateful** command is not in the configuration. If the ServerIron ADX is configured with the **server no-fast-stateful** command, the passive RTT information will be gathered on the remote site ServerIron ADX and sent out to the GSLB controller. If other Sever Load Balancing features such as L7 switching (CSW switching) are

configured on the remote site ServerIron ADX, the passive RTT information is also gathered and sent out to the GSLB controller. You can check the features on a ServerIron ADX using **show feature** command on a BP console. If "SLB only" is display as “ON,” that means that the ServerIron ADX will only process basic load balance traffic.

FIGURE 9 Passive RTT gathering


GSLB ServerIron
2. The GSLB ServerIron replies with the optimal IP address for the client.
LDNS
4. Site ServerIron reports RTT for client to GSLB ServerIron using GSLB protocol.
3. Site ServerIron uses passive RTT gathering to determine RTT.
1. Client sends a DNS query for www.brocade.com to LDNS. LDNS sends the query to the GSLB ServerIron.
Client
Site ServerIron

There are several advantages to the passive RTT gathering mechanism. Some of them are:

- RTT measurements are done passively by the Site ServerIron ADX using the existing traffic flow. No new traffic is introduced in the network to gather RTT.
- Measurements always reflect the RTT between the client and the Site ServerIron ADX, not the local DNS server (LDNS) of the client and the Site ServerIron ADX. This is an important advantage if the client and its LDNS server are not topographically close to each other.
- Since RTT is passively determined from the connection initiated by the client, the Site ServerIron ADX will always be able to gather RTT.

Although there are many advantages to using passive RTT gathering, this mechanism may not be adequate in some situations.

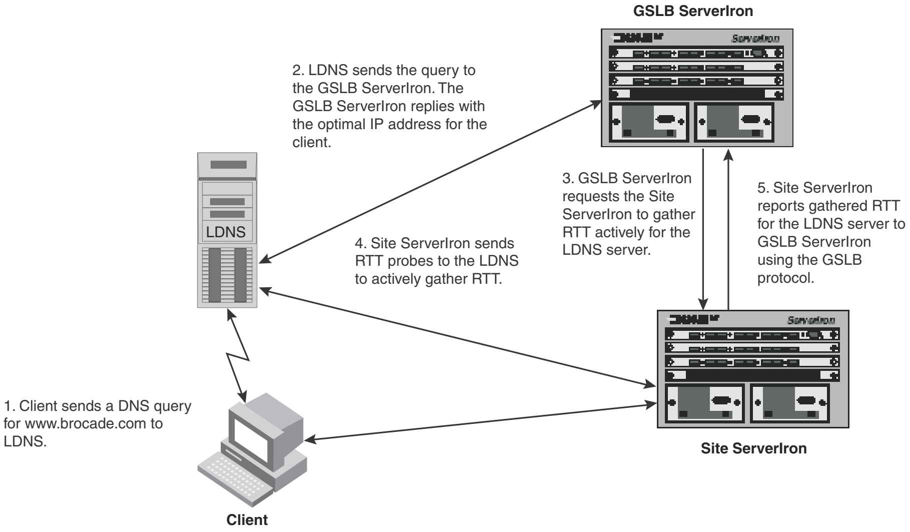
- If the client and its LDNS do not share the same network prefix, GSLB ServerIron ADX will not be able to use the passively gathered RTT values for IP address selection.
- Also, RTT can be gathered by a Site ServerIron ADX only if the client opens a connection to it. The GSLB ServerIron ADX needs to distribute a percentage of resolution requests to ensure that all the Site ServerIron ADXs have a chance to gather RTT.

Active RTT gathering

ServerIron ADX supports active RTT gathering where all Site ServerIron ADXs gather the RTT by sending probes to the client’s local DNS (LDNS) servers. They report this measured RTT to the GSLB controller using the GSLB protocol. The GSLB controller uses this RTT to select the best IP address for the client.

Active RTT is always measured between the Site ServerIron ADX and the client LDNS. This method of measuring RTT enables the GSLB ServerIron ADX to use this actively gathered RTT even if the client and its LDNS do not share the same network prefix.

FIGURE 10 Active RTT gathering


GSLB ServerIron
2. LDNS sends the query to the GSLB ServerIron. The GSLB ServerIron replies with the optimal IP address for the client.
LDNS
3. GSLB ServerIron requests the Site ServerIron to gather RTT actively for the LDNS server.
5. Site ServerIron reports gathered RTT for the LDNS server to GSLB ServerIron using the GSLB protocol.
4. Site ServerIron sends RTT probes to the LDNS to actively gather RTT.
1. Client sends a DNS query for www.brocade.com to LDNS.
Site ServerIron
Client

By default, the Site ServerIron ADXs actively gather RTT measurement by sending ICMP probes. In addition to ICMP probes, Site ServerIron ADXs can be configured to send DNS probes to gather RTT.

Each Site ServerIron ADX maintains an active RTT cache. This cache contains the LDNS host prefixes and LDNS host IP addresses that the Site ServerIron ADX received from the GSLB ServerIron ADX. When a Site ServerIron ADX receives an active RTT request from the GSLB ServerIron ADX, along with a list of LDNS host IP addresses, it compares the LDNS host IP address in the list to the LDNS prefixes in its active RTT cache. If the host prefix already exists in its active RTT cache, the Site ServerIron ADX refreshes that prefix entry. If it does not exist, then the Site ServerIron ADX creates a new entry for the LDNS prefix and LDNS host IP address. It also initiates RTT measurement for the prefix by sending a probe to that LDNS host.

The Site ServerIron ADX maintains a timestamp for each LDNS prefix in the active RTT cache. The timestamp indicates the last time the prefix was probed for RTT. If the time that has elapsed since the last probe is greater than the active RTT refresh interval on the Site ServerIron ADX, then the Site ServerIron ADX initiates a new RTT probe to the LDNS host for that prefix. Periodically refreshing the RTT ensures that the values accurately reflect the RTT between the LDNS host and the Site ServerIron ADX and takes into account any changes in the network conditions.

Support for both active and passive RTT

Brocade GSLB supports both active and passive RTT gathering.

Active RTT gathering is available on ServerIron ADXs running GSLB protocol version 3 or later. Use the **show gslb site** command to determine what protocol version a ServerIron ADX is running.

GSLB ServerIron ADXs periodically exchange version information with the Site ServerIron ADXs using the GSLB protocol. A protocol version number greater than or equal to 3 indicates that active RTT gathering is available in the software running on the ServerIron ADXs. ServerIron ADXs with a version less than 3 supports passive RTT gathering only.

GSLB ServerIron ADXs on which active RTT gathering is enabled is compatible with Site ServerIron ADXs that are running passive RTT gathering, and vice versa. You can have an active RTT gathering GSLB ServerIron ADX with some Site ServerIron ADXs running active RTT gathering and others that are running passive RTT gathering. You can also have a GSLB ServerIron ADX that supports only passive RTT gathering (for example. a ServerIron ADX) with the Site ServerIron ADXs that are running active RTT gathering. This characteristic helps you transition the ServerIron ADX on your network to active RTT gathering one ServerIron ADX at a time. Also, the transition can start with a GSLB ServerIron ADX or Site ServerIron ADXs.

By default, Site ServerIron ADXs that have active RTT gathering enabled gather RTT using passive and active RTT mechanisms. The Site ServerIron ADXs report only the actively gathered RTT to the GSLB ServerIron ADXs that have active RTT gathering enabled. They report passively gathered RTT values to GSLB ServerIron ADXs that do not support active RTT gathering. You can configure a Site ServerIron ADX to gather only active RTT.

NOTE
For passive round-trip-time gathering from remote site, the command "server no-fast-stateful" should be configured on the site.

Active RTT gathering issues and trade-offs

Active RTT gathering enables the GSLB ServerIron ADX to use the gathered RTT during selection of the best IP address, even if the client and its LDNS do not share the same network prefix. Actively gathered RTT values are gathered on-demand and made available on the GSLB ServerIron ADX for the selection process. However, there are some issues and trade-offs involved with active RTT gathering:

- Active RTT is always gathered between the Site ServerIron ADX and the LDNS. The underlying assumption here is that the RTT between Site ServerIron ADX and the LDNS is reasonably indicative of the RTT between the Site ServerIron ADX and the client.
- Site ServerIron ADXs actively gather RTT by sending probes. This characteristic introduces additional traffic into the network. You can control the amount of traffic by adjusting the frequency of the active RTT probes.
- The active RTT gathering load on the Site ServerIron ADXs varies, depending on the frequency of probing and other parameters. The higher the frequency of probing, the greater the accuracy and availability of the RTT, but the greater the load on the Site ServerIron ADX, the network traffic, and vice versa. You can control this by adjusting the frequency of the active RTT probes.
- If the active RTT probes are blocked on the LDNS by some security mechanisms, then the Site ServerIron ADX may not be able to gather RTT to that LDNS. To deal with this issue, Brocade GSLB feature allows you probe for RTT using both ICMP and DNS probes.

Enabling active RTT

Active RTT gathering is available on ServerIron ADX running protocol version 3 and higher; it is disabled by default on these ServerIron ADXs. Use the **show gslb site** command to determine if the ServerIron ADX is running protocol version 3 or higher. (See "Displaying RTT information" on page 152.) If it is, enable active RTT gathering on the GSLB ServerIron ADX by entering commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb active-rtt-gathering
```

Syntax: [no] gslb active-rtt-gathering

Once you enter this command on the GSLB ServerIron ADX, the GSLB ServerIron ADX performs a message exchange with each Site ServerIron ADX to determine if it is running a version that supports active RTT gathering. If it does, then the GSLB ServerIron ADX instructs the Site ServerIron ADX to enable active RTT gathering.

For a new deployment, it is generally helpful to start with minimum values for all active RTT parameters and a high value for active RTT cache interval. For example, you can configure the following on all active RTT controllers and Site ServerIron ADXs.

```
...
gslb active-rtt-query-interval 30
gslb agent-active-cache-interval 1800
gslb active-rtt-to-peer-interval 5
gslb agent-rtt-refresh-interval 30
...
```

Once you determine the active RTT is working correctly for the topology, you can experiment to determine the best values for that particular network/traffic.

Discarding passive RTT

Some of the Site ServerIron ADXs for a GSLB ServerIron ADX that has active RTT gathering enabled, may not support active RTT gathering. These Site ServerIron ADXs report passively gathered RTT to the GSLB ServerIron ADX. If you do not want the GSLB ServerIron ADX to process any passively gathered RTT, enter the following command on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb discard-passive-rtt
```

Syntax: [no] gslb discard-passive-rtt

Disabling passive RTT gathering

Once the GSLB instructs Site ServerIron ADXs to enable active RTT gathering, Site ServerIron ADXs use both active and passive methods to gather RTT values. Using the two methods allows a Site ServerIron ADX to communicate simultaneously with a GSLB ServerIron ADX that has active RTT enabled and another GSLB ServerIron ADX that does not have active RTT gathering enabled (for example, ServerIron ADX). The actively gathered RTT value is reported only to GSLB ServerIron ADX that supports active RTT gathering. The passively gathered RTT is reported only to GSLB ServerIron ADX that supports passive RTT gathering.

However, if all the GSLB ServerIron ADXs to which the Site ServerIron ADX is communicating with support active RTT gathering, then you can disable passive RTT gathering on the Site ServerIron ADXs by entering the following command.

```
SITE-ServerIronADX# configure terminal
SITE-ServerIronADX(config)# gslb disable-rtt-gathering
```

Syntax: [no] gslb disable-rtt-gathering

Configuring active RTT parameters

Configuring active RTT query message interval

The active RTT query message interval refers to the time intervals at which the GSLB ServerIron ADX sends the list of LDNS addresses to the Site ServerIron ADXs. These are the LDNS hosts for which the Site ServerIron ADXs need to actively gather the RTT.

To configure the active RTT query message interval, enter the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb active-rtt-query-interval 60
```

Syntax: [no] gslb active-rtt-query-interval <*value*>

Enter a value between 30-21600 seconds for <*value*>. The default is 60 seconds.

Specifying how often to report the active RTT

Site ServerIron ADX must report the actively gathered RTT to the GSLB ServerIron ADX periodically. To specify the interval, enter the following on the Site ServerIron ADX.

```
SITE-ServerIronADX# configure terminal
SITE-ServerIronADX(config)# gslb active-rtt-to-peer-interval 30
```

Syntax: [no] gslb active-rtt-to-peer-interval <*value*>

Enter a number from 5-1800 seconds for <*value*>. The default is 60 seconds.

Configuring the cache interval for active RTT prefix

A Site ServerIron ADX on which active RTT gathering is enabled maintains an active RTT cache. The cache contains the LDNS host prefixes and LDNS host IP addresses that the Site ServerIron ADX received from the GSLB ServerIron ADX. The entries in the active RTT cache are refreshed each time the GSLB ServerIron ADX sends an active RTT probing request for that LDNS prefix. If they are not refreshed, the entries are aged out from the active RTT cache after a specified time. This duration is referred to as the cache interval.

To configure the cache interval for an active RTT prefix on the Site ServerIron ADX, enter the following command.

```
SITE-ServerIronADX# configure terminal
SITE-ServerIronADX(config)# gslb agent-active-cache-interval 300
```

Syntax: [no] gslb agent-active-cache-interval <*value*>

Enter a value from 120-3600 seconds for <*value*>. The default is 600 seconds.

NOTE
This command affects only the active RTT cache maintained by the Site ServerIron ADX. It does not apply to and has no relation to the client prefix cache maintained by the GSLB controller.

Configuring the active RTT refresh interval

The Site ServerIron ADX maintains a timestamp for each of the LDNS prefixes in its active RTT cache. The time stamp indicates the last time RTT was probed. If the time that has elapsed since the last probe is greater than the RTT refresh interval on the Site ServerIron ADX, then the Site ServerIron ADX initiates a new RTT measurement probe to the LDNS host for that prefix. Periodically refreshing the RTT ensures that the values for a LDNS host reflect the RTT between the LDNS host and the Site ServerIron ADX correctly.

To configure the active RTT refresh interval on the Site ServerIron ADX, enter the following command.

```
SITE-ServerIronADX# configure terminal
SITE-ServerIronADX(config)# gslb agent-rtt-refresh-interval 40
```

Syntax: [no] gslb agent-rtt-refresh-interval <*value*>

Enter a value from 30-1800 seconds for <*value*>. The default is 600 seconds.

Setting the RTT algorithm modes

The GSLB ServerIron ADX on which active RTT gathering is enabled may be communicating with Site ServerIron ADXs that support active RTT gathering and other Site ServerIron ADXs that support only passive RTT gathering (for example, ServerIron ADX). Therefore, depending on the network configuration and the topology, some of the RTT values that have been gathered for a prefix may be passive RTT values while others may be active RTT values.

For example, GSLB ServerIron ADX has three Site ServerIron ADXs. Each of the Site ServerIron ADX reported RTT values for prefix 201.53.x.x:

- Site ServerIron ADX-1 (1.1.1.102) supports active RTT gathering and reported an actively probed RTT value of 7ms for prefix 201.53.x.x.
- Site ServerIron ADX-2 (1.1.1.117) supports passive RTT gathering and reported a passively gathered RTT value of 12 ms for prefix 201.53.x.x.
- Site ServerIron ADX-3 (1.1.1.18) supports passive RTT gathering and reported a passively gathered value of 18ms for 201.53.x.x.

The following will be recorded for prefix 201.53.x.x in the prefix cache of the GSLB ServerIron ADX.

Prefix: 201.53.0.0, prefix length = 16

ServerIron ADX= 1.1.1.102, rtt = 7ms, source = active (probe type = ICMP)

ServerIron ADX= 1.1.1.117, rtt = 12ms, source = passive (probe type = Not applicable)

ServerIron ADX= 1.1.1.118, rtt = 18ms, source = passive, (probe type = Not applicable)

With active RTT gathering implementation, you can create a GSLB policy and indicate which values in the cache will be used when selecting the optimal IP address:

- **RTT algorithm selection based only on passive RTT values (Mode 1)**: Only RTT values that were gathered passively by Site ServerIron ADXs will be used in determining the optimal IP address.
- **RTT algorithm selection based only on active RTT values (Mode 2):** Only RTT values that were gathered actively by Site ServerIron ADXs will be used in determining the optimal IP address.
- **RTT algorithm selection based on both active and passive RTT values (Mode 3):** All RTT values will be used when determining the optimal IP address, whether they were gathered using active or passive RTT measurements.

In the example above, assume that the GSLB ServerIron ADX is configured as Mode 2. Also assume that this GSLB ServerIron ADX is providing GSLB for *www.foo.com* where the IP addresses for this domain are IP-1, IP-2, and IP-3. IP-1 is a VIP on ServerIron ADX-1. IP-2 is a VIP on ServerIron ADX-2. IP-3 is a VIP on ServerIron ADX-3.

If a DNS resolution request comes from LDNS 201.53.10.1, then GSLB ServerIron ADX uses only the RTT information for IP-1 which is configured on ServerIron ADX 1.1.1.102 (rtt = 7ms, source = active). Since the GSLB ServerIron ADX in configured as Mode 2, only actively reported RTT values are used during the selection. The RTTs for IP-2 and IP-3 are not used since the source of these RTTs is passive.

The RTT algorithm mode can be configured globally in a global GSLB policy or locally in a host-level GSLB policy. Placing the modes in different policies allows you to use different RTT algorithm modes for different hosts. The default RTT algorithm mode for a global or host level GSLB policy is Mode 1.

Using only passive RTT

To configure a global GSLB policy to use only passive RTT values for RTT algorithm (Mode 1), enter commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB_ServerIronADX(config)# gslb policy
GSLB-ServerIronADX(config-gslb-policy)# round-trip-time active-rtt
use-passive-rtts-only
```

To configure a host-level GSLB policy to use only passive RTT values for RTT algorithm (Mode 1), enter commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb-host-policy test
GSLB-ServerIronADX(config-gslb-host-policy-test)# round-trip-time active-rtt
use-passive-rtts-only
```

Syntax: **round-trip-time active-rtt use-passive-rtts-only**

Using only active RTT

To configure a global GSLB policy to use only active RTT values for RTT algorithm (Mode 2), enter commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB_ServerIronADX(config)# gslb policy
GSLB-ServerIronADX(config-gslb-policy)# round-trip-time active-rtt
use-active-rtts-only
```

To configure a host-level GSLB policy to use only active RTT values for RTT algorithm (Mode 2), enter commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb-host-policy test
GSLB-ServerIronADX(config-gslb-host-policy-test)# round-trip-time active-rtt
use-active-rtts-only
```

Syntax: **round-trip-time active-rtt use-active-rtts-only**

Using both active and passive RTT

To configure a global GSLB policy to use both passive and active RTT values for RTT algorithm (Mode 3), enter commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb policy
GSLB-ServerIronADX(config-gslb-policy)# round-trip-time active-rtt
use-active-and-passive-rtts
```

To configure a host-level GSLB policy to use both passive and active RTT values for RTT algorithm (Mode 3), enter commands such as the following

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb-host-policy test
GSLB-ServerIronADX(config-gslb-host-policy-test)# round-trip-time active-rtt
use-active-and-passive-rtts
```

Syntax: **round-trip-time active-rtt use-active-and-passive-rtts**

Probes for RTT gathering

By default, a Site ServerIron ADX on which active RTT gathering is enabled uses an ICMP prober to gather active RTT values. In addition to ICMP prober, a DNS prober can also be enabled on the Site ServerIron ADX. The DNS prober gathers RTT actively by sending a DNS query to the LDNS server and calculating RTT for that LDNS server when it receives the corresponding DNS response.

The DNS prober is disabled by default. If you enable the DNS prober, then the Site ServerIron ADX gathers RTT using both ICMP prober and DNS prober and reports measurements from their probes to the GSLB controller.

Accepting DNS RTT measurements

If DNS prober is enabled on the Site ServerIron ADX, then the GSLB ServerIron ADX receives the DNS RTT measurements in addition to the ICMP RTT measurements from that Site ServerIron ADX. By default, the GSLB ServerIron ADX does not use the DNS RTT measurements reported by Site ServerIron ADXs.

You need to enable the GSLB ServerIron ADX to accept DNS RTT measurements reported by Site ServerIron ADXs. Also, you need to indicate if a fallback mechanism should be used between the DNS RTT measurements and the ICMP RTT measurements. If the fallback mechanism is disabled, ICMP RTT value is used as the primary RTT value. If the fallback mechanism is enabled, DNS RTT value is used as the primary RTT value and ICMP RTT is used as the secondary RTT value.

During selection of the best IP address for a client, the GSLB ServerIron ADX will always use the primary RTT value. If the primary RTT value has failed or is unavailable, then the GSLB ServerIron ADX will use the backup RTT value only if the fallback mechanism on the GSLB ServerIron ADX has been enabled.

To enable the GSLB ServerIron ADX to accept DNS RTT measurements and to enable fallback mechanism, enter the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb dns-probe enable-fallback
```

Syntax: **gslb dns-probe enable-fallback**

To enable the GSLB ServerIron ADX to accept DNS RTT measurements but to disable fallback mechanism, enter commands such as the following on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb dns-probe disable-fallback
```

Syntax: **gslb dns-probe disable-fallback**

If neither of these commands is configured, then the GSLB ServerIron ADX will not use any DNS probe measurement reported by the Site ServerIron ADXs and will use only the RTT values reported by the ICMP probe for the best IP address selection.

Enabling the DNS prober

To enable the DNS prober on the Site ServerIron ADX, enter the following on the Site ServerIron ADX.

```
Site-ServerIronADX# configure terminal
Site-ServerIronADX(config)# gslb agent-dns-prober
```

Syntax: **gslb agent-dns-prober**

Sending DNS probes on a different port

By default Site ServerIron ADX sends DNS probes on port 9990. To send the probe on a different port, enter commands such as the following on the Site ServerIron ADX.

```
Site-ServerIronADX# configure terminal
Site-ServerIronADX(config)# gslb udp-probe-port 10000
Site-ServerIronADX(config)# reload
```

Syntax: **gslb udp-probe-port** <*port-number*>

Enter a number for <*port-number*>.

NOTE
A reload on the ServerIron ADX is required for this command to take effect.

Aging out prefixes when ICMP probe fails

You can instruct the Site ServerIron ADX to quickly age out a cache prefix for an LDNS host from the active RTT cache if an ICMP probe or a DNS probe to an LDNS host fails. Once the prefix is aged out, the Site ServerIron ADX collects RTT values from a different LDNS host for that prefix after it receives the next prefix or LDNS-host list update from the GSLB ServerIron ADX containing this same prefix.

To quickly age out prefixes from the active RTT cache on the Site ServerIron ADX when the *ICMP* probe to that LDNS host fails, enter the following on the Site ServerIron ADX.

```
SITE-ServerIronADX# configure terminal
SITE-ServerIronADX(config)# gslb agent-fast-age-icmp-fail
```

Syntax: **[no] gslb agent-fast-age-icmp-fail**

Aging out prefixes when DNS probe fails

To quickly age out prefixes from the active RTT cache on the Site ServerIron ADX when the *DNS* probe to those LDNS hosts fail, configure the following on the Site ServerIron ADX.

```
SITE-ServerIronADX# configure terminal
SITE-ServerIronADX(config)# gslb agent-fast-age-dns-fail
```

Syntax: **[no] gslb agent-fast-age-dns-fail**

If both the ICMP and DNS fast-aging commands are enabled on the Site ServerIron ADX, then failure of either ICMP or DNS probes will quickly age out LDNS prefixes from the active RTT cache. Typically you should enable only one of these commands. Follow the guidelines below to determine which command to enable:

- If you want DNS RTT measurements to be the primary source of RTT and DNS prober is enabled on the Site ServerIron ADX, then enable the **gslb agent-fast-age-dns-fail** command if LDNS prefixes need to quickly age out if a DNS probe fails.
- If you want ICMP RTT measurements to be the only source of RTT and DNS prober is not enabled on the Site ServerIron ADX, then enable the **gslb agent-fast-age-icmp-fail** command if LDNS prefixes need to quickly age out if an ICMP probe fails.
- If you want the LDNS prefix to be aged out when either DNS or ICMP prober fails, then enable both commands on the Site ServerIron ADX.
- If no fast aging is desired, then do not enter either of the commands.

Active RTT gathering and high availability support

Brocade GSLB with active RTT gathering will operate in all High Availability (HA) configurations supported in earlier software releases.

To ensure that active RTT gathering is synchronized between devices that are in an HA configuration, GSLB active RTT gathering does the following:

- If two GSLB ServerIron ADXs are in an HA configuration and both have active RTT gathering enabled, then each active RTT gathering Site ServerIron ADX reports the actively gathered RTT information to both the GSLB ServerIron ADXs. This ensures that the standby GSLB ServerIron ADX receives the actively gathered RTT information and is able to immediately use this information if the primary GSLB ServerIron ADX fails over.
- If two Site ServerIron ADXs are in an HA configuration and have active RTT gathering enabled, then the GSLB ServerIron ADX sends the active RTT gathering request with the list of LDNS hosts that are to be probed to both the Site ServerIron ADXs. Each of the Site ServerIron ADXs in the HA configuration actively gathers RTT measurements from the LDNS hosts in the list and reports information to the GSLB ServerIron ADX. This ensures that the GSLB ServerIron ADX receives RTT information for both the Site ServerIron ADXs. If the primary Site ServerIron ADX fails over and the standby Site ServerIron ADX takes over, the GSLB ServerIron ADX will already have the RTT information for the standby Site ServerIron ADX. The GSLB ServerIron ADX will be able to immediately select the best IP address based on the information it has.

Displaying RTT information

Displaying the RTT gathering mechanism

To view the RTT gathering mechanism for a Site ServerIron ADX, enter the following command on the GSLB ServerIron ADX.

```
ServerIronADX# show gslb site
SITE: local
 Enhanced RTT smoothing: OFF
ServerIronADX:  1.1.1.102:
state: SELF
Protocol Version: 3
distributed health-chk
Active RTT gathering: ON
 Current num.  Session   CPU load  Preference  Location  Connection
 sessions      util(%)   (%)       (0-255)               Load-Avg
           24        0          6        128  N-AM           --
 Virtual IPs:
         1.1.1.101(A)
SITE: test2
 Enhanced RTT smoothing: OFF
ServerIronADX:  1.1.1.117:
state: CONNECTION ESTABLISHED
Protocol Version: 1
non-distributed health-chk
Active RTT gathering: OFF
 Current num.  Session   CPU load  Preference  Location  Connection
 sessions      util(%)   (%)       (0-255)               Load-Avg
            5        0          1        128  N-AM           --
 Virtual IPs:
          1.1.1.93(A)
```

In the example above, Site ServerIron ADX 1.1.1.102 has protocol version 3 and has active RTT gathering enabled. Site ServerIron ADX 1.1.1.117 has protocol version 1; active RTT gathering is not available on that ServerIron ADX.

Syntax: **show gslb site**

This command also shows the protocol version number that the Site ServerIron ADX is running. A protocol version number greater than or equal to 3 indicates that the active RTT gathering is available on that Site ServerIron ADX.

Displaying the active RTT gathering configuration

To view the active RTT gathering configuration parameters, enter the following command.

```
ServerIronADX# show gslb active-rtt-info
Controller Information:
-----------------------
 Active RTT gathering: ENABLE
 Discard Passive RTT recvd. from agent: DISABLE
 Interval to send active rtt query buffer to agent = 60 sec
 DNS probe = Disable, Fallback=Disable
Agent Information:
------------------
 Num active RTT peers = 1
 Num passive RTT peers = 0
 Agent active rtt cache interval = 600 sec
 Agent active rtt refresh interval = 600 sec
 Num valid prefixes in agent active rtt tree = 0
 Interval to send gathered active rtt to controller = 60 sec
 Disable passive RTT gathering on agent: NO
 Num RTT queries in progress = 0
 Fast age on ICMP RTT probe fail = 0
 Agent DNS prober = DISABLE
 DNS probe port: configured = 9990, in-use = 9990
 Num DNS RTT queries in progress = 0
 Fast age on DNS RTT probe fail = 0
```

Syntax: show gslb active-rtt-info

In the sample output above, the ServerIron ADX is both a GSLB ServerIron ADX as well as a Site ServerIron ADX. If the ServerIron ADX is a GSLB ServerIron ADX, information only for the GSLB controller will be displayed. Likewise, if the ServerIron ADX is only a Site ServerIron ADX, only information for the Agent will be displayed.

TABLE 9 Show GSLB active RTT information

This field...	Displays...
Controller	This area shows information about the GSLB ServerIron ADX.
Active RTT gathering	State of active RTT gathering mechanism on the GSLB ServerIron ADX: Enabled or Disabled.
Discard Passive RTT recvd. from agent	Shows the GSLB ServerIron ADX is configured to discard any passive RTTs received from Site ServerIron ADXs.
Interval to send active rtt query buffer to agent	The interval at which the GSLB ServerIron ADX sends query buffer containing LDNS prefixes to Site ServerIron ADXs.
DNS probe	Indicates if controller has been configured to accept RTT information gathered using DNS probes. Possible values: ENABLE or DISABLE
Fallback	Indicates if fallback mechanism has been enabled on the controller. If enabled, controller will use DNS RTT information. If this is not available, it will use ICMP RTT information. If disabled, controller will only use ICMP RTT information.
Agent	This area shows information about the Site ServerIron ADX.
Num active RTT peers	Number of passive RTT GSLB ServerIron ADXs for which this ServerIron ADX is a Site ServerIron ADX.

TABLE 9 Show GSLB active RTT information (Continued)

This field...	Displays...
Num passive RTT peers	Number of active RTT GSLB ServerIron ADXs for which this ServerIron ADX is a Site ServerIron ADX.
Agent active rtt cache interval	The cache interval for a prefix in the Site ServerIron ADX's active RTT cache.
Agent active rtt refresh interval	The interval at which the Site ServerIron ADX refreshes the RTT value for LDNS prefixes in its active RTT cache.
Num valid prefixes in agent active rtt tree	Number of LDNS prefixes in the Site ServerIron ADX active RTT cache.
Interval to send gathered active rtt to controller	Interval at which the Site ServerIron ADX reports the actively gathered RTT to the GSLB controller.
Disable passive RTT gathering on agent	Shows if passive RTT gathering is disabled on the Site ServerIron ADX.
Num RTT queries in progress	Number of ICMP RTT probes in progress on the Site ServerIron ADX.
Fast age on ICMP RTT probe fail	Shows if a LDNS prefix in the Site ServerIron ADX's active RTT cache is aged out immediately if ICMP probes to that LDNS fail. A value of 1 or greater means that the ICMP probes are aged out immediately.
Agent DNS prober	Indicates if DNS prober is enabled or disabled on the Site ServerIron ADX.
DNS probe port	**configured**: Indicates the port number configured for sending out DNS probes **in-use**: Indicates the port number being currently used for sending out DNS probes. If the configured and in-use values are different, then the DNS probe port was changed, but the ServerIron ADX has not been reloaded. **NOTE:** DNS probe port command needs a reload to take effect.
Num DNS RTT queries in progress	Number of DNS RTT probes in progress on the Site ServerIron ADX.
Fast age on DNS RTT probe fail	Shows if a LDNS prefix in the Site ServerIron ADX active RTT cache is aged out immediately when DNS probes to that LDNS fail. A value of 1 or greater means that the DNS probes are aged out immediately.

Displaying the RTT information of a client IP address

The GSLB ServerIron ADX maintains a cache of RTT information received from the site ServerIron ADXs through the GSLB protocol. You can display the RTT information the GSLB ServerIron ADX has for a client IP address.

To display the RTT information for a particular client, enter a command such as the following:

```
ServerIronADX# show gslb cache 1.1.1.42
prefix length = 20, prefix = 1.1.0.0, region = N-AM
prefix source = active-rtt-update,
  site = cupertino,  ServerIronADX = (1.1.1.115),  rtt = 20 (x100 usec) *A   >D
(OK) backup rtt = 16 (x100 usec) (OK)
  site = local,  ServerIronADX = (1.1.1.102),  rtt = 65535 (x100 usec) *A   >D
(FAL) backup rtt = 8 (x100 usec) (OK)
```

Syntax: **show gslb cache** <*ip-address*>

This output shows that the prefix 1.1.0.0, prefix length = 20 was created due to an active RTT update from the Site ServerIron ADX. The primary RTT reported for this prefix by Site ServerIron ADX 1.1.1.115 is 2000 usec, the source is active RTT gathering and the probe method is DNS. The backup RTT is 1600usec and the method is ICMP probes.

The output of the command has been enhanced to also display the following:

- Prefix Source
- The source of an RTT entry can be active, passive, or unknown
- The method of gathering shows the type of probe used: ICMP, DNS, or not applicable
- The primary and backup RTT values. A value that appears for the backup RTT is of significance only if the fallback mechanism is configured on the GSLB ServerIron ADX.
- Whether or not the probe was successful.

This field...	Displays...
Prefix length	The length of the prefix
Prefix source	Displays why the prefix entry was created
region	Geographic region for the prefix
Site	Name of the Site ServerIron ADX
ServerIron ADX	IP address of the Site ServerIron ADX
rtt	The primary RTT reported for the prefix in usec.
*	The source of an RTT entry (denoted by *) for a prefix. Source can be one of the following: • A = Active • P = Passive • U = Unknown
>	The method of gathering the RTT is displayed in the output. The method can be: • I = ICMP probe • D = DNS probe • N = Not applicable
backup rtt	The backup RTT reported for the prefix in usec. This value is significant only if the fallback mechanism is configured on the GSLB ServerIron ADX.
( )	Result of the RTT probe: • OK: RTT probe is successful • FAL: RTT probe has failed or RTT to the LDNS server is unavailable

Displaying the RTT algorithm mode

To display the RTT algorithm mode, enter the following command.

```
GSLB-ServerIronADX#show gslb policy
  Default metric order: DISABLE
  Metric processing order:
                1-Round trip time between remote ServerIronADX and client
                2-Least response selection
  DNS active-only: ENABLE   DNS best-only: ENABLE   DNS override: DISABLE
  DNS cache-proxy: DISABLE  DNS transparent-intercept: DISABLE
  DNS cname-detect: DISABLE  Modify DNS response TTL: ENABLE
  DNS TTL: 10 (sec), DNS check interval: 30 (sec)
  Remote ServerIronADX status update period: 30 (sec)
  Remote ServerIronADX health-status update period: 5 (sec)
  Session capacity threshold: 90%  Session availability tolerance: 10%
  Round trip time tolerance: 10%, round trip time explore percentage: 5%
  Round trip time cache prefix: 20, round trip time cache interval: 600 (sec)
  Round trip time cache age refresh: DISABLE
  Round trip time algorithm selection:  USE PASSIVE ONLY
  Connection load: DISABLE
  Weighted Site Metric: DISABLE     Weighted IP Metric: DISABLE
  Active Bindings Metric: DISABLE
```

Syntax: show gslb policy

This command has been enhanced to display the RTT algorithm mode.

The following host-level policy **show** commands have been enhanced to also display the RTT algorithm mode:

- **show gslb policy host-policy-all**
- **show gslb policy host-policy-name** <*policy-name*>

For example, enter a command such as the following:

```
ServerIronADX#show gslb policy host-policy-name test-mode
GSLB POLICY: test-mode
  Default metric order: ENABLE
  Metric processing order:
                1-Server health check
                2-Remote ServerIronADX’s session capacity threshold
                3-Round trip time between remote ServerIronADX and client
                4-Geographic location
                5-Remote ServerIronADX’s available session capacity
                6-Least response selection
  DNS active-only: DISABLE  DNS best-only: DISABLE
  Session availability tolerance: 10%
  Round trip time tolerance: 10
  Round trip time algorithm selection:  USE ACTIVE AND PASSIVE
  Connection load: DISABLE
  Weighted Site Metric: DISABLE     Weighted IP Metric: DISABLE
  Active Bindings Metric: DISABLE
```

GSLB affinity for high availability

The GSLB Affinity feature configures the GSLB ServerIron ADX to always prefer a specific Site ServerIron ADX for queries from clients (or client LDNS servers) whose addresses are within a configured IP prefix. To configure affinity, you associate a site ServerIron ADX with an IP prefix. When the GSLB ServerIron ADX receives a query from a client (or client LDNS server) whose IP address is within this configured prefix, the GSLB ServerIron ADX examines the DNS reply for a virtual IP address (VIP) configured on the ServerIron ADX associated with this IP prefix. It selects this VIP as the optimal IP address for the querying client (or client LDNS).

The GSLB Affinity feature allows you to associate an IP prefix with a ServerIron ADX. Consider the example where, ServerIron ADX-1 is in a high availability (HA) configuration with ServerIron ADX-2. You associate an IP prefix 1.1.1.0/24 with ServerIron ADX-1 using the existing affinity configuration command. You also configure VIP-1 on ServerIron ADX-1 where it is in the active state, and on ServerIron ADX-2 where it is in the standby state. VIP-1 is also one of the IP addresses configured for domain *www.foo.com* for which the GSLB ServerIron ADX is providing GSLB.

If a client in the 1.1.1.0/24 network sends a query for *www.foo.com*, the GSLB ServerIron ADX selects VIP-1 as the best IP address for the client, because the IP prefix 1.1.1.0/24 has been associated with ServerIron ADX-1 and VIP-1 is active on ServerIron ADX-1.

Now if a failover occurs between ServerIron ADX-1 and ServerIron ADX-2, VIP-1 becomes active on ServerIron ADX-2 and standby on ServerIron ADX-1. If a client (or client LDNS) in the 1.1.1.0/24 network queries for *www.foo.com*, the GSLB ServerIron ADX will no longer select VIP-1 as the optimal address based on the affinity configuration. The reason is that the affinity for 1.1.1.0/24 is configured for ServerIron ADX-1 but VIP-1 is no longer active on ServerIron ADX-1 but is active on ServerIron ADX-2. Since there is no affinity definition associated with ServerIron ADX-2, GSLB ServerIron ADX is unable to use it for best IP address selection.

There is flexibility in defining GSLB high availability groups that include ServerIron ADXs in any supported HA topologies. You can configure affinity similar to that described above (that is, an IP address prefix will be associated with a ServerIron ADX). However if your configure an HA group for the ServerIron ADXs, GSLB ServerIron ADX will be able to detect the HA peer for the ServerIron ADX configured in the affinity definition. Also, GSLB ServerIron ADXs will be able to use the affinity definition for both the ServerIron ADXs in the HA group.

For example, in the example described above with ServerIron ADX-1 and ServerIron ADX-2 in HA configuration, IP prefix 1.1.1.0/24 is associated with ServerIron ADX-1. Also, an HA group consisting of ServerIron ADX-1 and ServerIron ADX-2 can now be configured. When a client (or client LDNS) in the 1.1.1.0/24 network queries for *www.foo.com*, the GSLB ServerIron ADX selects VIP-1 as the best IP address no matter where it is active (on ServerIron ADX-1 or on ServerIron ADX-2, its peer ServerIron ADX configured in the HA group).

Configuring an HA group

Before configuring a GSLB HA Group, make sure the Site ServerIron ADXs that you want to place in the HA group have been configured.

Once Site ServerIron ADXs have been configured, you can configure an HA group that consists of two Site ServerIron ADXs by entering the following commands on the GSLB ServerIron ADX.

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb ha-group 1.1.1.55 1.1.1.65
ServerIronADX(config)# end
```

Syntax: [no] gslb ha-group *<ServerIron ADX-IP-address-1> <ServerIron ADX-IP-address-2>*

Enter the IP address of the two Site ServerIron ADXs in a HA group for *<ServerIron ADX-IP-address-1>* and *<ServerIron ADX-IP-address-2>.* Currently, you can specify only two Site ServerIron ADXs in a HA group. You can configure as many HA groups as needed, but a Site ServerIron ADX can only be in one HA group at a time.

You can associate the affinity definition for a client (or client LDNS prefix) with either of the ServerIron ADXs in the HA group. GSLB ServerIron ADX automatically uses the affinity definition for both ServerIron ADXs in the HA group.

NOTE
When running a ServerIron ADX with a switch image, the management IP address must be configured before configuring a local site. This is true for configuring for a fresh box or changing an IP address.

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb site local
ServerIronADX(config-gslb-site-local)# si 1.1.1.102
ServerIronADX(config-gslb-site-local)# exit
ServerIronADX(config)# gslb site test
ServerIronADX(config-gslb-site-test)# si 1.1.1.9
ServerIronADX(config-gslb-site-test)# exit
ServerIronADX(config)# gslb ha-group 1.1.1.102 1.1.1.9
ServerIronADX(config)# gslb affinity
ServerIronADX(config-gslb-affinity)# prefer 1.1.1.9 for 1.1.1.0/24
ServerIronADX(config-gslb-affinity)# end
```

In this example, the configured affinity definition is used for ServerIron ADX 1.1.1.102 and ServerIron ADX 1.1.1.9 since they belong to the same GSLB HA group.

Enabling dynamic detection

You can also enable dynamic detection of HA Site ServerIron ADXs on the GSLB ServerIron ADX. If Site ServerIron ADX-1 and Site ServerIron ADX-2 are in high availability configuration and distributed health-checking is enabled between the Site ServerIron ADX and the GSLB ServerIron ADX, then the GSLB ServerIron ADX will be able to dynamically determine that they are an HA pair. However it will be not be able to dynamically detect these ServerIron ADXs as an HA pair, if one of the following occurs:

- One of the Site ServerIron ADXs loses connection to the GSLB ServerIron ADX and does not re-establish connection to the GSLB ServerIron ADX.
- Distributed health checking is not supported or not enabled between the GSLB ServerIron ADX and these Site ServerIron ADXs.

HA groups should be configured and dynamic detection should be configured only as a backup mechanism.

NOTE
Dynamic detection is an optional configuration and is not needed when HA groups are configured.

To enable dynamic detection of HA pairs, complete the following tasks.

1. Make sure you configure HA groups for the ServerIron ADX. (Refer to “Configuring an HA group” on page 157.)
2. Enable dynamic detection as a backup mechanism by entering commands such as the following on the GSLB ServerIron ADX.

   ```
   ServerIronADX# configure terminal
   ServerIronADX(config)# gslb dynamic-peer-detect
   ServerIronADX(config)# end
   ```

   Syntax: [no] gslb dynamic-peer-detect

Displaying HA information

Displaying all HA groups

To view all the configured HA groups on the GSLB ServerIron ADX, enter the following command on the GSLB ServerIron ADX.

```
ServerIronADX# show gslb ha-group-info

 Configured GSLB HA groups:
* GSLB HA group: {ServerIron 1.1.1.55, ServerIron 1.1.1.65}
   Virtual IPs for ServerIron 1.1.1.55: None
    Virtual IPs for ServerIron 1.1.1.65: None
* GSLB HA group: {ServerIron 1.1.1.102, ServerIron 1.1.1.9}
    Virtual IPs for ServerIron 1.1.1.102:
         1.1.1.101(A)
    Virtual IPs for ServerIron 1.1.1.9:
          1.1.1.101(S)
```

Syntax: show gslb ha-group-info

Displaying the HA peer for a site

To view the configured HA peer for a Site ServerIron ADX, enter the following command on the GSLB ServerIron ADX.

```
GSLB-ServerIronADX# show gslb site local

SITE: local
 Enhanced RTT smoothing: OFF

ServerIronADX:  1.1.1.102:
state: SELF
Protocol Version: 4
distributed health-chk
Active RTT gathering: NO
Authenticate: NO, Encrypt: NO
Cfg HA peer: ServerIronADX 1.1.1.9

 Current num.  Session   CPU load  Preference  Location  Connection
 sessions      util(%)   (%)       (0-255)               Load-Avg
           18        0         99         128  N-AM           --

 Virtual IPs:
         1.1.1.101(A)
```

Syntax: **show gslb site** <*site-name*>

The field "Cfg HA peer" shows the configured HA peer Site ServerIron ADX for this Site ServerIron ADX.

Displaying the dynamically detected HA pairs

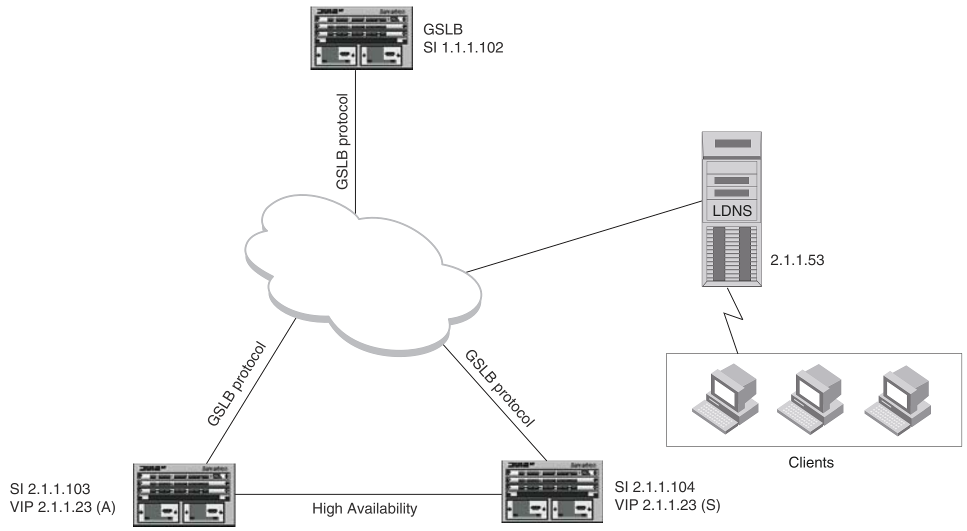
To view the dynamically detected ServerIron ADX HA pairs, use the following command on the GSLB ServerIron ADX.

```
ServerIronADX#show gslb dns detail

ZONE: gslb1.com
HOST: www:
(Global GSLB policy)
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*       1.1.1.133: dns real-ip DOWN   N-AM     --   --    0 (0%)
*        1.1.1.44: dns real-ip DOWN   N-AM     --   --    0 (0%)
*       1.1.1.101: dns v-ip    ACTIVE N-AM      0    0    7 (100%)
                  Active Bindings: 1
                  site: local, weight:   0, ServerIronADX: 1.1.1.102
                  HA Peer ServerIronADX(dynamic): 1.1.1.105
                  session util:   0%, avail. sessions: 5999981
                  preference: 128
                  Metric counter (count [selection-metric]):
                  3[health-check]
                  Affinity selection count = 4

*       1.1.1.116: dns real-ip DOWN   N-AM     --   --    0 (0%)
```

Syntax: **show gslb dns detail**

The output above shows that for VIP 1.1.1.101, the GSLB ServerIron ADX dynamically detected Site ServerIron ADXs 1.1.1.102 and 1.1.1.105 to be in a HA configuration. In particular, it detected that VIP 1.1.1.101 is in active state on ServerIron ADX 1.1.1.102 and is in standby state on ServerIron ADX 1.1.1.105.

FIGURE 11 GSLB affinity for HA



ServerIron ADX 1.1.1.102 is a GSLB ServerIron ADX that is providing GSLB for domain *www.foo.com*. One of the IP addresses for ww.foo.com is 2.1.1.23.

ServerIron ADX 2.1.1.103 and ServerIron ADX 2.1.1.104 are Site ServerIron ADXs. The GSLB ServerIron ADX and the Site ServerIron ADXs communicate using the GSLB protocol. ServerIron ADX 2.1.1.103 and ServerIron ADX 2.1.1.104 are in a high availability configuration. VIP 2.1.1.23 is configured on ServerIron ADXs 2.1.1.103 and 2.1.1.104.

On the GSLB ServerIron ADX, configure a HA group consisting of ServerIron ADX 2.1.1.103 and 2.1.1.104 as follows.

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb ha-group 2.1.1.103 2.1.1.104
ServerIronADX(config)# end
```

Next, associate an affinity definition for client (or client LDNS) network 2.1.1.0/24 with ServerIron ADX 2.1.1.104 on the GSLB ServerIron ADX as follows.

```
GSLB-ServerIronADX(config)#gslb affinity
GSLB-ServerIronADX(config-gslb-affinity)#prefer 2.1.1.104 for 2.1.1.0/24
GSLB-ServerIronADX(config-gslb-affinity)#end
```

View the configured HA group using the following command.

```
GSLB-ServerIron ADX#show gslb ha-group-info

 Configured GSLB HA groups:
* GSLB HA group: {ServerIronADX 2.1.1.103, ServerIronADX 2.1.1.104}

    Virtual IPs for ServerIronADX 2.1.1.103:
         2.1.1.23(A)
    Virtual IPs for ServerIronADX 2.1.1.104:
          2.1.1.23(S)
```

In this example, VIP 2.1.1.23 is active (A) on ServerIron ADX 2.1.1.103 and standby (S) on ServerIron ADX 2.1.1.104.

Client LDNS 2.1.1.53 sends a DNS request to GSLB ServerIron ADX for *www.foo.com*. GSLB ServerIron ADX rearranges the DNS reply as follows.

1. It checks if there is any affinity definition associated with the client LDNS network. In this example, it finds that there is a definition associating network 2.1.1.0/24 with ServerIron ADX 2.1.1.104. So it checks if there is any IP address in the reply which is a VIP configured on ServerIron ADX 2.1.1.104 and is in the active (A) state on that ServerIron ADX.
2. Since it does not find any such VIP, it then checks if ServerIron ADX 2.1.1.104 is a part of GSLB HA group. In this example, it is a part of a HA group and its HA peer is ServerIron ADX 2.1.1.103.
3. It then checks if there is any IP address in the reply that is a VIP on 2.1.1.103. It finds IP address 2.1.1.23 in the DNS reply that is a VIP in the active (A) state on ServerIron ADX 2.1.1.103 and selects this as the best IP address for client LDNS 2.1.1.53.

GSLB optimization

A site ServerIron ADX sends a list of GSLB enabled VIPs to the GSLB controller on a periodic basis. If distributed health checks is enabled on the site ServerIron ADX, then this list would also include the health status of the VIP ports.

The following two procedures are used to optimize GSLB processes:

- "Optimized VIP list processing" on page 162.)
- "Increased VIP support per site and reduced CPU usage on GSLB controller" on page 162)

Optimized VIP list processing

The GSLB controller can optionally be enabled to process the VIPlist from the controller in a more optimal manner. This mechanism reduces CPU usage on controller.

The feature can be enabled by issuing following command at the global config level.

```
ServerIronADX(config)# gslb process-vip-list-optimize
```

Syntax: **[no] gslb process-vip-list-optimize**

NOTE
This command requires a reload to take effect.

Increased VIP support per site and reduced CPU usage on GSLB controller

Through use of the VIP List Optimize feature the maximum number of GSLB-enabled VIPs supported per site is 1024 VIPs per site.

Use the following commands on controller and site to avail this functionality.

1. On controller, enable VIP list process optimization by issuing the following command at global config level.

   ```
   ServerIronADX(config)# gslb process-vip-list-optimize
   ServerIronADX(config)# write memory
   ServerIronADX(config)# reload
   ```

   NOTE
   A system reload is required after enabling the **gslb process-vip-list-optimize** command.

2. Under a site definition on the controller, add the **si** <*si-ip-address*> **optimized-dist-hcheck** command.

   ```
   ServerIronADX(config)# gslb site sunnyvale
   ServerIronADX(config-gslb-site-sunnyvale)# si-name si-1 100.1.1.1
   ServerIronADX(config-gslb-site-sunnyvale)# si 100.1.1.1 optimized-dist-hcheck
   ```

   Syntax: [no] si <*ip-address*> **optimized-dist-hcheck**

   The **si** <*ip-address*> **optimized-dist-hcheck** helps the controller identify the site that has the VIP list process optimization enabled.

   NOTE
   If have not completed step 1 on the GSLB controller (configured **gslb process-vip-list-optimize** saved the configuration and reloaded the device), the message: `"Please enable hashing to optimize vip list processing and reload!"` will be displayed on the GSLB controller SI when you configure this command on the Site SI and reload.

3. Issue the **gslb send-vip-list-optimize** command on the Site ServerIronADX.

   ```
   Site-ServerIronADX(config)# gslb send-vip-list-optimize
   Site-ServerIronADX(config)# write memory
   Site-ServerIronADX(config)# reload
   ```

   Syntax: [no] gslb send-vip-list-optimize

   NOTE
   A system reload is required after enabling this feature.

4. If site ServerIronADX is hosting more than 217 GSLB enabled VIPs, then you need to disable the site ServerIronADX from sending active binding information. Issue the following command.

   ```
   Site-ServerIronADX(config)# gslb dont-send-active-bindings
   ```

   Syntax: [no] gslb dont-send-active-bindings

5. Issue the **show gslb site** command to determine if optimization of the VIP list processing is enabled for a Site ServerIron ADX, as shown in the following:

```
ServerIronADX# show gslb site

SITE: site-1
 Enhanced RTT smoothing: OFF
SI:  68.87.24.37:
state: CONNECTION ESTABLISHED
Protocol Version: 1
distributed health-chk
Active RTT gathering: NO
Secure Authenticate/Encrypt: NO, Optimized dist hcheck: YES,
 Current num.  Session   CPU load  Preference  Location  Connection
 sessions      util(%)   (%)       (0-255)               Load-Avg
          160        0          4         128  N-AM           --

 Virtual IPs:
       68.87.9.213(A)       68.87.8.212(A)
       68.87.7.211(A)       68.87.6.210(A)
       68.87.5.209(A)       68.87.4.208(A)
       68.87.3.207(A)       68.87.2.206(A)
         3.3.3.233(A)      68.87.64.202(A)
      68.87.64.215(A)      68.87.64.214(A)
      68.87.64.213(A)      68.87.64.216(A)
      68.87.64.210(S)      68.87.64.209(S)
      68.87.64.208(S)      68.87.64.204(S)
      68.87.64.137(S)      68.87.64.180(S)
      68.87.64.183(S)      68.87.64.196(S)
      68.87.64.164(A)      68.87.64.132(S)
```

Syntax: **show gslb site**

The **optimized dist hcheck** parameter in the **show gslb site** output indicates if VIP list process optimization is enabled on ServerIron ADX.

Configuration example

On controller ServerIron ADX, configure the following commands.

```
ServerIronADX(config)# gslb process-vip-list-optimize
ServerIronADX(config)# gslb site site-1
ServerIronADX(config-gslb-site-site-1)# si 5.5.5.1  optimized-dist-hcheck
ServerIronADX(config-gslb-site-site-1)# exit
ServerIronADX(config)# gslb site site-2
ServerIronADX(config-gslb-site-site-2)# si 68.87.1.2  optimized-dist-hcheck
ServerIronADX(config-gslb-site-site-2)# exit
ServerIronADX(config)# write memory
ServerIronADX(config) #reload
```

On the site ServerIron ADX, configure the following commands.

```
ServerIronADX(config)# gslb send-vip-list-optimize
ServerIronADX(config)# write memory
ServerIronADX(config)# reload
```

NOTE
A **reload** is required if the GSLB optimization features are enabled on the GSLB controller or a GSLB site ServerIron ADX.

Guidelines and recommendations for using this feature

We recommend that you observe the following guidelines when using this feature:

- The GSLB controller and ServerIron ADX Side functionality (remote or local) should not be configured on the same ServerIron ADX.
- Domain IPs should be VIPs rather than real IP hosts to minimize the health-check load on the GSLB controller.
- Anytime a site ServerIron ADX state is changed from optimized to non-optimized (or vise versa) you must reload the controller.
- If the GSLB optimization feature is enabled on the GSLB controller, then it is recommended to not enable SLB for other services (enabling other services can cause resource problems).
- The GSLB controller will support maximum of 2048 GSLB enabled VIPs from all site ServerIrons. You must ensure that maximum number of GSLB enabled VIPs received from all sites does not exceed 2048.
- To reduce the CPU usage, especially when there are many zones and GSLB enabled VIPs configured, the GSLB optimization features should be enabled on both the GSLB controller and GSLB site ServerIron ADXs as described in “Increased VIP support per site and reduced CPU usage on GSLB controller” on page 162
- When a Site ServerIron ADX has more than 256 SLB VIPs the controller health-status interval should be set to 5 seconds (default value) or longer.

Displaying GSLB information

Displaying site information

You can display the following site information:

- ServerIron ADX name and management IP address
- Site name (displayed only if you display information for all sites rather than an individual site)
- State of the GSLB protocol connection between GSLB ServerIron ADX and site ServerIron ADX
- Number of sessions in the ServerIron ADX’s session table
- The percentage of the total number of sessions the ServerIron ADX can maintain that are in use
- The percentage of the ServerIron ADX’s CPU that is actively engaged in SLB and other activities
- The numeric preference value for this site ServerIron ADX
- The geographic location of the ServerIron ADX
- The virtual IP addresses (VIPs) configured on the ServerIron ADX

To display information for the sites you have configured on the GSLB ServerIron ADX, use either of the following methods.

To display information for all the configured sites, enter the following command at any level of the CLI.

```
ServerIronADX(config)# show gslb site
SITE: sunnyvale
ServerIronADX: slb-1 209.157.22.209:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
       500000       50         35  128         N-AM
 Virtual IPs:
     209.157.22.227(A)         209.157.22.103(A)
ServerIronADX: slb-2 209.157.22.210:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
            1        0         16  128         N-AM
 Virtual IPs:
     209.157.22.227(S)
SITE: atlanta
ServerIronADX: slb-1 192.108.22.111:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
       750000       75         41  128         N-AM
 Virtual IPs:
    209.157.22.227(A)          209.157.22.104(A)
ServerIronADX: slb-1 192.108.22.111:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
            1       0         16   128         N-AM
 Virtual IPs:
    209.157.22.227(S)
```

The following example shows information displayed when the connection-load metric is enabled.

```
ServerIronADX(config-gslb-policy)# show gslb site

SITE: two
ServerIronADX:  1.1.1.2:
state: CONNECTION ESTABLISHED

 Current num.  Session   CPU load  Preference  Location  Connection
 sessions      util(%)   (%)       (0-255)               Load-Avg
            6        0         19         128  N-AM            30

 Virtual IPs:
          1.1.1.12(A)

 Connection Load (Seconds:AvgLoad):
   5:36  10:34  15:32  20:31  25:30  30:28
```

Syntax: **show gslb site** [<*name*>]

The <*name*> parameter specifies a site name.

To display information about the GSLB site called “sunnyvale” and the ServerIron ADXs providing SLB within those sites, enter the following command.

```
ServerIronADX(config)# show gslb site sunnyvale
ServerIronADX: slb-1 209.157.22.209:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
       500000       50         35  128         N-AM
 Virtual IPs:
     209.157.22.227(A)
ServerIronADX: slb-2 209.157.22.210:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
            1        0         16  128         N-AM
 Virtual IPs:
     209.157.22.227(S)
```

The **show gslb site** display shows the following information.

TABLE 10 Global SLB site information

This field...	Displays...
ServerIron ADX name and IP address	For each ServerIron ADX, the first item of information listed is the name and management IP address. This is the information you specified when you added the ServerIron ADX to the site.
SITE	Indicates the site name of the ServerIron ADX. **NOTE:** This field appears only when you enter the **show gslb site** command without specifying a site name.
ServerIron ADX	Indicates the site ServerIron ADX name and management IP address.
State	The state of the GSLB protocol connection between the GSLB ServerIron ADX and the site ServerIron ADX. The state can be one of the following: • ATTEMPTING CONNECTION: The GSLB ServerIron ADX is still trying to establish a GSLB connection with the site ServerIron ADX. • CONNECTION ESTABLISHED: The GSLB ServerIron ADX has established a GSLB connection with the site ServerIron ADX. • SELF: The GSLB ServerIron ADX is also this site ServerIron ADX.
Current num. sessions	The number of sessions in the ServerIron ADX’s session table. A session is a one-way connection to or from a real server. This information is reported by the site ServerIron ADX. **NOTE:** The number of sessions in the table does not necessarily match the number of active sessions on the real servers. This can occur if the session table contains sessions that are no longer active but have not yet timed out.
Session util (%)	The percentage of available sessions that are in use. This is the percentage of the total number of sessions the ServerIron ADX can maintain that are in use. For example, if the ServerIron ADX can maintain 1 million sessions (the default session capacity) and the session table contains 500,000 session entries, the session utilization is 50%. This information is reported by the site ServerIron ADX.
CPU load (%)	The percentage of the ServerIron ADX’s CPU that is actively engaged in SLB and other activities. This information is reported by the site ServerIron ADX.

TABLE 10 Global SLB site information (Continued)

This field...	Displays...
Preference	The numeric preference value for this site ServerIron ADX. The preference can be used by the GSLB policy to select a site. Refer to "Site ServerIron ADX's administrative preference" on page 11. This information is configured on the GSLB ServerIron ADX.
Location	The geographic location of the ServerIron ADX. The location is based on the ServerIron ADX's management IP address and can be one of the following: • ASIA • EUROPE • N-AM: North America • S-AM: South America NOTE: If you explicitly identified the geographic location, the value you specified appears instead of a value based on the IP address. Refer to "Configuring a site" on page 19.
Virtual IPs	The virtual IP addresses (VIPs) configured on the ServerIron ADX. This information is reported by the site ServerIron ADX. The letter in parentheses at the end of each address indicates whether the ServerIron ADX is an active or standby ServerIron ADX for that address. The letter can be A (active) or S (standby). Unless the ServerIron ADX is configured along with a partner ServerIron ADX for Symmetric Server Load Balancing, the value is always A. If a number appears following the A or S, a host range (the unlimited VIP feature) is configured on the VIP. The number indicates the number of hosts in the host range. NOTE: The GSLB ServerIron ADX does not necessarily provide global SLB for all the VIPs configured on the site ServerIron ADXs. The GSLB provides global SLB only for the VIPs that correspond to the DNS zone names you configure the GSLB ServerIron ADX to load balance.
Connection Load	The average load at each connection-load sampling interval in the most recent set of sample intervals. In the example above, the connection load metric is configured to use six samples, at 5-second intervals. The sampling intervals and the average new-connection load at each interval are shown. On this site ServerIron ADX, the average new-connection load for the last five seconds is 36, the average new-connection load for the last 10 seconds is 34, the average new-connection load for the last 15 seconds is 32, the average new-connection load for the last 20 seconds is 31, and so on. Any time you enter the command for this site ServerIron ADX, the average load for the last 30 seconds is shown.

Displaying real server information

rshow 209.157.22.209 server real

Generally, remote ServerIron ADXs in a GSLB configuration are themselves configured with real servers and virtual servers. The real servers are the actual file servers for which the remote ServerIron ADX provides load balancing. The virtual servers are the logical IP addresses that are published instead of the real server IP addresses.

The GSLB protocol allows you to query the site ServerIron ADXs for configuration information as well as the session and CPU information used by the GSLB policy. You can view detailed configuration information and statistics for the site ServerIron ADX, from the GSLB management console. You can display the following information:

- Real server configuration
- Virtual server configuration
- Port binding information (for the bindings between TCP/UDP ports on the real servers and the virtual server that represents the real servers)
- Session statistics for sessions between clients and the real servers

To display real server information for the real servers configured on a remote ServerIron ADX, enter commands such as the following at any level of the GSLB ServerIron ADX's CLI.

```
ServerIronADX(config)# rshow 209.157.22.209 server real
Real Servers Info
Name : rs1                                          Mac-addr: abcd.5a11.d042
IP:10.10.10.1      Range:1    State:Active          Wt:1     Max-conn:1000000
Port    State    Ms CurConn TotConn Rx-pkts  Tx-pkts  Rx-octet   Tx-octet   Reas
----    -----    -- ------- ------- -------  -------  --------   --------   ----
ftp     enabled  0  0       0       0        0        0          0          0
http    enabled  0  0       0       0        0        0          0          0
default unbnd    0  0       0       0        0        0          0          0
Server  Total       0       0       0        0        0          0          0
Name : rs2                                          Mac-addr: abcd.5a11.d043
IP:10.10.10.2      Range:1    State:Active          Wt:1     Max-conn:1000000
Port    State    Ms CurConn TotConn Rx-pkts  Tx-pkts  Rx-octet   Tx-octet   Reas
----    -----    -- ------- ------- -------  -------  --------   --------   ----
ftp     enabled  0  0       0       0        0        0          0          0
http    enabled  0  0       0       0        0        0          0          0
default unbnd    0  0       0       0        0        0          0          0
Server  Total       0       0       0        0        0          0          0
```

The command in this example displays real server configuration information for the remote ServerIron ADX with management IP address 209.157.22.209. As shown in Figure 1 on page 4, this ServerIron ADX is part of the "sunnyvale" site and is configured to load balance two real servers. In this example, the real servers are named rs1 and rs2.

Syntax: **rshow** <*remote-ip-addr*> **server real** | **virtual** | **session** | **bind**

The <*remote-ip-addr*> parameter specifies the remote ServerIron ADX's management IP address.

The **real** | **virtual** | **session** | **bind** parameter specifies the information you want to display:

- **real**: displays real server information. This option is equivalent to entering the show server real command on the remote ServerIron ADX.
- **virtual**: displays virtual server information. This option is equivalent to entering the show **server virtual-name-or-ip** command on the remote ServerIron ADX.
- **session**: displays session statistics. This option is equivalent to entering the show server session command on the remote ServerIron ADX.
- **bind**: displays port binding information. This option is equivalent to entering the show server bind command on the remote ServerIron ADX.

Displaying DNS zone and hosts

To display information about the DNS zones and host names that you have configured the GSLB ServerIron ADX to globally load balance, use either of the following methods.

NOTE
There are two examples of this command line output shown below. The output differs depending on the ServerIron ADX device you are using and the software release installed on the ServerIron ADX.

NOTE
If you also want to display information about the site and ServerIron ADX on which a VIP is configured, use the **show gslb dns detail** command instead. Refer to "Displaying detailed DNS information" on page 172.

To display information about all the DNS zones and host applications configured on the GSLB ServerIron ADX, enter the following command at any level of the CLI.

```
ServerIronADX(config)# show gslb dns zone
                                                    Flashback  DNS resp.
                                                    delay      selection
                                                    (x100us)   percentage
                                                    TCP  APP   (%)
* 209.157.22.227: dns        v-ip    ACTIVE N-AM.     6   60   40
* 209.157.22.228: dns        v-ip    ACTIVE N-AM.     3   30   60
* 210.224.100.5:  dns        real-ip DOWN   ASIA     --   --     0
* 201.100.100.6:  dns        real-ip DOWN   S-AM.    --   --     0
* 213.34.100.4:   dns        real-ip DOWN   EUROPE   --   --     0

HOST: ftp:
                                                    Flashback  DNS resp.
                                                    delay      selection
                                                    (x100us)   percentage
                                                    TCP  APP   (%)
* 209.157.22.103: dns        v-ip    ACTIVE N-AM.     6   60   40
* 209.157.22.104: dns        v-ip    ACTIVE N-AM.     3   30   60
* 210.224.100.7:  dns        real-ip DOWN   ASIA     --   --     0
* 201.100.100.8:  dns        real-ip DOWN   S-AM.    --   --     0
* 213.34.100.9:   dns        real-ip DOWN   EUROPE   --   --     0
```

Syntax: **show gslb dns zone** [<*name*>]

The <*name*> parameter specifies the zone name.

To display GSLB information for a specific DNS zone, enter a command such as the following:

```
ServerIronADX(config)# show gslb dns zone brocade.com
```

The information is the same as the information displayed when you do not specify a zone name, except the ZONE field is unneeded and thus does not appear.

This display shows the following information.

TABLE 11 GSLB zone and host application information

This field...	Displays...
ZONE	The zone name. The name that appears here is the name you specified when you configured the zone information. NOTE: This field appears only if you do not specify the zone name when you display the information. If you specify the zone name, information for only that zone is displayed.
HOST	The host name. The name that appears here is the name you specified when you configured the host information.
IP addresses	The column of IP addresses lists the IP addresses the authoritative DNS server associated with the host name in the DNS reply. These are the servers that contain the content for the host. In this example, the servers contain the content for www.brocade. After evaluating the addresses using the GSLB policy, the GSLB ServerIron ADX marks each address that passes the algorithm with an asterisk (*). An IP address that does not have an asterisk in front of it has not passed the GSLB algorithm and cannot be selected as the "best" site. NOTE: If DNS override is enabled, only the addresses configured in the host's IP list have asterisks and are valid choices for the best site. Refer to "Enabling DNS override" on page 33.
Source	The value following each server IP address indicates how the ServerIron ADX learned the address. This field can have one of the following values: • cfg: The address is one that you associated with the host as part of the DNS override feature. Refer to "Enabling DNS override" on page 33. • d/c: The address was learned from the DNS server and also is one that you associated with the host. • dns: The address was learned from the DNS server. In the example above, the ServerIron ADX learned about all the IP addresses associated with the zone name from the DNS server; thus, the source is listed as "dns".
Type	The next value indicates the type of address, which can be one of the following: • v-ip: The address is a VIP configured on a ServerIron ADX. • real-ip: The address is a real server.
State	The state of the server. The ServerIron ADX determines the state based on the results of the Layer 7 health checks sent to the server. The ServerIron ADX sends Layer 7 health checks for each host application you associate with the zone. The state can be one of the following: • ACTIVE: The server passed the Layer 4 and Layer 7 health checks and is presumed to be available. • DOWN: The server failed a health check. If any of the health checks are failed, the GSLB ServerIron ADX disqualifies this site from being the "best" site. NOTE: If the server has multiple applications, all the applications must pass the health check. NOTE: The ServerIron ADX also uses the results of the health check, if the server passes the check, in the TCP and App columns under FlashBack Delay, described below.

TABLE 11 GSLB zone and host application information (Continued)

This field...	Displays...
Location	The geographic location of the server. The location is based on the IP address and can be one of the following: • ASIA • EUROPE • N-AM: North America • S-AM: South America The GSLB ServerIron ADX can use this information when comparing the servers in order to select the "best" ones for the client. The GSLB ServerIron ADX prefers servers within the client's geographic region over servers in other geographic regions.
FlashBack Delay (x100us)	The round-trip time for a health check sent by the GSLB ServerIron ADX to the host application on the server. The GSLB ServerIron ADX can use this information when comparing the servers in order to select the "best" ones for the client. The GSLB ServerIron ADX prefers servers with lower round-trip times to those with higher round-trip times. The value in the TCP column indicates the round-trip time of the Layer 4 health check to the TCP port. The value in the App column indicates the round-trip time for the Layer 7 health check. NOTE: A single value is displayed even if the zone has multiple host applications. If the FlashBack values (round-trip times) differ, the slowest times are displayed.
DNS resp. selection counters Count	The number of times the GSLB ServerIron ADX has selected this server as the "best" server and thus placed the server's IP address at the top of the list in DNS replies.
DNS resp. selection percentage (%)	The percentage of times the GSLB ServerIron ADX has selected this server as the "best" server and thus placed the server's IP address at the top of the list in DNS replies.

Displaying detailed DNS information

You can display all the information displayed by the **show gslb dns zone** command, plus information about the site and the ServerIron ADX on which a VIP is configured, by entering the **show gslb dns detail** command.

This command is especially useful for sites that are configured for Symmetric Server Load Balancing. For information about this load balancing feature, see High Availability.

This example assumes that the ServerIron ADXs at the sunnyvale site are each configured with two VIPs for the "www" host and two VIPs for the "ftp" host in the brocade.com domain:

- VIPs 209.157.22.100 and 209.157.22.101 are configured on both ServerIron ADXs for the "www" host.
- VIPs 209.157.22.102 and 209.157.22.103 are configured on both ServerIron ADXs for the "ftp" host.

The same VIPs are configured on both ServerIron ADXs, but only one of the ServerIron ADXs is actively load balancing for a particular VIP. The other ServerIron ADX is the standby for that VIP and assumes load balancing duties for the VIP only if the other ServerIron ADX becomes unavailable. The default active ServerIron ADX for a particular VIP is determined by the priority you assign to the VIP when you are configuring Symmetric SLB.

In this example, ServerIron ADX slb-1 is the active ServerIron ADX for VIPs 209.157.22.100 and 109.157.22.101 and ServerIron ADX slb-2 is the default active ServerIron ADX for VIPs 209.157.22.103 and 209.157.22.104. Although this example has both VIPs for a host active on the same ServerIron ADX, you can just as easily configure the VIPs so that both ServerIron ADXs have active VIPs for the same host.

NOTE
This example does not show the information for the atlanta site.

The text shown in bold type in the example is the information that is not displayed by the **show gslb dns zone** command

```
ServerIronADX# show gslb dns detail

ZONE: b.c
HOST: a:
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP   APP    Count (%)
*        4.4.4.11: dns v-ip    DOWN   N-AM     --    --    6 (18%)
                  site: four, ServerIronADX: 4.4.4.1
                  session util:   0%, avail. sessions: 524286
                  preference: 125
*        1.1.1.11: dns v-ip    ACTIVE N-AM      0     0    6 (18%)
                  site: local, ServerIronADX: 1.1.1.1
                  session util:   0%, avail. sessions: 5999985
                  preference: 150
*        2.2.2.11: dns v-ip    DOWN   N-AM     --    --    15 (46%)
                  site: two, ServerIronADX: 2.2.2.1
                  session util:   0%, avail. sessions: 524286
                  preference: 250
*        3.3.3.11: dns real-ip DOWN   N-AM     --    --    5 (15%)
```

Syntax: **show gslb dns detail** [<*name*>]

The <*name*> parameter specifies a zone name.

TABLE 12 Global SLB zone and host application information

This field...	Displays...
site	Indicates the site name of the ServerIron ADX.
ServerIron	Indicates the site ServerIron ADX name and management IP address.
session util	Indicates the percentage of the ServerIron ADX session capacity that is in use. This information is reported by the site ServerIron ADX using the GSLB protocol.
preference	The numeric preference value for this site ServerIron ADX. The preference can be used by the GSLB policy to select a site. Refer to "Site ServerIron ADX's administrative preference" on page 11.
avail. sessions	Indicates the number of unused sessions in the ServerIron ADX's session table.

For descriptions of the other information displayed by the **show gslb dns detail** command, refer to "Displaying DNS zone and hosts" on page 170.

Displaying metric information

You can show the following information:

- The metrics that were used to select a given site as the best site.
- For each of the GSLB metrics that have been used to select the site, the number of times that metric was the deciding factor in selection of the site.

To view metric information, enter the following command.

```
ServerIronADX# show gslb dns detail

ZONE: gslb.com
HOST: www:
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)
*        1.1.1.24: dns real-ip DOWN   N-AM     --   --    5 (19%)
*       1.1.1.101: dns v-ip    ACTIVE N-AM      0    0    8 (30%)
                  site: sunnyvale, ServerIronADX: 1.1.1.102
                  session util:   0%, avail. sessions: 524277
                  preference: 128
                  Metric counter (count [selection-metric]):
                  1[health-check]  3[round-robin]  4[least-response]
*        1.1.1.22: dns real-ip DOWN   N-AM     --   --    7 (26%)
*        1.1.1.23: dns real-ip ACTIVE N-AM    276   18    6 (23%)
```

Syntax: **show gslb dns detail** [<*name*>]

This command's output is enhanced to show the following information:

- The metrics that were used to select a given site as the best site.
- For each of the GSLB metrics that have been used to select the site, the number of times that metric was the deciding factor in selection of the site.

The metric statistics are displayed under the Metric counter line. In this example, site 1.1.1.101 has been selected as the best site a total of eight times. This is shown in the DNS resp. selection counters column. The health-check metric was used once to select site, the round robin selection metric was used three times to select the site, and the least-response metric was used four times to select the site.

If the site has not been selected yet as the best site, the line under Metric counter says "Not selected yet".

Displaying the default GSLB policy

To display the default GSLB policy, enter the following command.

```
ServerIronADX(config)# show gslb default
  Default metric order: ENABLE
  Metric processing order:
                1-Server health check
                2-Remote ServerIronADX's session capacity threshold
                3-Round trip time between remote ServerIronADX and client
                4-Geographic location
                5-Remote ServerIronADX's available session capacity
                6-Server flashback speed
                7-Least response selection

  DNS active-only: DISABLE   DNS best-only: DISABLE   DNS override: DISABLE
  Modify DNS response TTL: ENABLE
  DNS TTL: 10 (sec), DNS check interval: 30 (sec)
  Remote ServerIronADX status update period: 30 (sec)
  Session capacity threshold: 90%, session capacity tolerance: 10%
  Round trip time tolerance: 10%, round trip time explore percentage: 5%
  Round trip time cache prefix: 20, round trip time cache interval: 120 (sec)
  Flashback appl-level delay tolerance: 10%, TCP-level delay tolerance: 10%
```

Syntax: **show gslb default**

This display shows the following information.

TABLE 13 GSLB policy information

This field...	Displays...
Default algorithm	Indicates whether this policy is in effect. The value can be one of the following: • Disable • Enable If the state is Disable, then a user-configured policy is in effect instead.
Metric processing order	Indicates the order in which the selection metrics are applied to the server addresses in the DNS reply. For information about the metrics, refer to "GSLB policy" on page 6.
DNS active-only	Indicates whether the GSLB ServerIron ADX removes IP addresses from the DNS response if those addresses fail a health check. This field can have one of the following values: • DISABLE: The ServerIron ADX does not remove the IP addresses from the DNS response. • ENABLE: The ServerIron ADX removes IP addresses that fail a health check from the DNS response.
DNS best-only	Indicates whether you have configured the ServerIron ADX to remove all IP addresses except the "best" address from DNS replies. This field can have one of the following values: • DISABLE: The ServerIron ADX does not remove all addresses except the best one. • ENABLE: The ServerIron ADX removes all addresses except the best one. NOTE: Even when this feature is enabled, if the GSLB policy does not result in selection of a best address, the DNS reply can still contain more than one address. For more information, refer to "Removing all addresses except the best address" on page 31.

TABLE 13 GSLB policy information (Continued)

This field...	Displays...
DNS override	Indicates whether DNS override is enabled. DNS override replaces the addresses in a DNS reply with the "best" address from a list of addresses you configure. This field can have one of the following values: • **DISABLE**: The ServerIron ADX does not replace the addresses in DNS replies with an address from a list you configure. • **ENABLE**: The ServerIron ADX replaces the addresses in DNS replies with an address from a list you configure. For more information about DNS override, refer to "Enabling DNS override" on page 33.
Modify DNS response TTL	Indicates whether the GSLB ServerIron ADX modifies the TTL in the DNS records in DNS responses before sending the responses to the client's DNS server. This field can have one of the following values: • **DISABLE**: The ServerIron ADX does not modify the TTLs. • **ENABLE**: The ServerIron ADX modifies the TTLs.
DNS TTL	Indicates the value (number of seconds) to which the GSLB ServerIron ADX changes the TTL in each DNS record in the DNS responses before sending them to the client's DNS server. **NOTE:** If the Modify DNS response TTL field contains "DISABLE", the ServerIron ADX does not change the TTLs, regardless of the value in this field.
DNS check interval	Indicates how frequently the GSLB ServerIron ADX refreshes its zone and host information with DNS servers.
Remote ServerIron ADX status update period	Indicates how frequently the remote ServerIron ADXs send status updates to the GSLB ServerIron ADX through the GSLB protocol.
Session capacity threshold	Specifies how close to its maximum session capacity the site ServerIron ADX (remote ServerIron ADX) can be and still be eligible as the best site for the client. If a site ServerIron ADX exceeds the threshold, the site ServerIron ADX is ineligible to be the best site.
Session capacity tolerance	Specifies the percentage by which the number of available sessions on the site ServerIron ADX can differ from the number of available sessions on another site ServerIron ADX and still be considered an equally good site. Refer to "Site ServerIron ADX's available session capacity tolerance" on page 10.
Round trip time tolerance	Specifies the percentage by which the RTT for one site can differ from the RTT for another site without this metric resulting in selection of one site over the other.
Round trip time explore percentage	Indicates the percentage of client requests from a given network for which the GSLB ServerIron ADX intentionally ignores the RTT metric when evaluating the IP addresses in the DNS reply. The explore percentage prevents the ServerIron ADX from continually biasing its site selection based on the first ServerIron ADX to return RTT information. Refer to "Modifying round-trip time values" on page 53.
Round trip time cache prefix	Indicates the length (number of significant bits) of entries in the GSLB ServerIron ADX's IP address cache. The prefix determines the extent to which IP addresses are aggregated into entries in the cache.
Round trip time cache interval	Indicates how many seconds the GSLB ServerIron ADX keeps an unrefreshed RTT cache entry in its cache before the entry ages out.

TABLE 13 GSLB policy information (Continued)

This field...	Displays...
Flashback appl-level delay tolerance	Indicates the percentage of difference that can exist between application level FlashBack response times for two sites, without the ServerIron ADX preferring one site over the other based on this metric.
TCP-level delay tolerance	Indicates the percentage of difference that can exist between Layer 4 FlashBack response times for two sites, without the ServerIron ADX preferring one site over the other based on this metric.

Displaying the user-configured GSLB policy

To display the user-configured GSLB policy, enter the following command.

```
ServerIronADX(config)# show gslb policy
  Default metric order: ENABLE
  Metric processing order:
                1-Server health check
                2-Remote ServerIronADX's session capacity threshold
                3-Round trip time between remote ServerIronADX and client
                4-Geographic location
                5-Remote ServerIronADX's available session capacity
                6-Server flashback speed
                7-Least response selection

  DNS active-only: DISABLE   DNS best-only: DISABLE   DNS override: DISABLE
  Modify DNS response TTL: ENABLE
  DNS TTL: 10 (sec), DNS check interval: 30 (sec)
  Remote ServerIronADX status update period: 30 (sec)
  Session capacity threshold: 90%, session capacity tolerance: 10%
  Round trip time tolerance: 10%, round trip time explore percentage: 5%
  Round trip time cache prefix: 20, round trip time cache interval: 120 (sec)
  Flashback appl-level delay tolerance: 10%, TCP-level delay tolerance: 10%
```

Syntax: **show gslb policy**

In this example, the default order of the policy metrics is in effect. Metrics that are disabled by default (such as the administrative preference) are not listed.

In the following example, the order has been changed, two of the metrics have been disabled, and the administrative preference has been enabled.

```
ServerIronADX(config)# show gslb policy
  Default metric order: DISABLE
  Metric processing order:
                1-Round trip time between remote ServerIronADX and client
                2-Remote ServerIronADX's session capacity threshold
                3-Remote ServerIronADX's available session capacity
                4-Server flashback speed
                5-Remote ServerIronADX's preference value
                6-Least response selection

  DNS active-only: DISABLE   DNS best-only: DISABLE   DNS override: DISABLE
  Modify DNS response TTL: ENABLE
  DNS TTL: 10 (sec), DNS check interval: 30 (sec)
  Remote ServerIronADX status update period: 30 (sec)
  Session capacity threshold: 90%, session capacity tolerance: 10%
  Round trip time tolerance: 10%, round trip time explore percentage: 5%
  Round trip time cache prefix: 20, round trip time cache interval: 120 (sec)
  Flashback appl-level delay tolerance: 10%, TCP-level delay tolerance: 10%
```

For a description of the information shown by this command, refer to “Displaying the default GSLB policy” on page 175.

Displaying RTT information

The GSLB ServerIron ADX maintains a cache of RTT information received from the site ServerIron ADXs through the GSLB protocol. You can display the RTT information the GSLB ServerIron ADX has related to a client IP address. To display the RTT information, specify a potential client address, as shown in the following example.

```
ServerIronADX(config)# show gslb cache 209.157.0.0
prefix length = 20, prefix = 209.157.0.0, region = N-AM
prefix source =             client-query

brocade.com:
  site = sunnyvale,  ServerIronADX = slb-1(209.157.22.209),  rtt = 5 (x100 usec)
  site = atlanta,  ServerIronADX = slb-1(192.108.22.112),  rtt = 10 (x100 usec)
```

The command in this example shows the RTT prefix information the GSLB ServerIron ADX has related to client IP address 209.156.100.100. In this case, the GSLB ServerIron ADX has two RTT entries for zone *www.brocade.com*.

Syntax: **show gslb cache** <*ip-addr*>

The <*ip-addr*> command specifies a site address.

The following example shows information for a user-configured static entry.

```
ServerIronADX(config)# show gslb cache 192.168.2.1
prefix length = 24, prefix = 192.168.2.0, region = N-AM
prefix source = static, client-query
www.brocade.com:
  site = atlanta,  ServerIronADX = slb-1(192.108.22.111),  rtt = 5 (x100 usec)
```

This example shows the RTT prefix cache entry that contains site IP address 192.1678.2.1. The prefix source line indicates that the prefix cache entry that matches the site address was added statically. Notice that a prefix cache entry can have more than one source. In this case, the prefix was statically configured but a specific entry (listed below under the domain name "*www.brocade.com*") was created when the GSLB ServerIron ADX received RTT information from the site ServerIron ADX for a site address within the prefix.

In the following example, a statically generated entry that the GSLB ServerIron ADX created is displayed. The statically generated entries have an 8-bit prefix, whereas the prefix for dynamic entries is 20 bits long by default.

```
ServerIronADX(config)# show gslb cache 61.1.1.1

prefix length = 8, prefix = 60.0.0.0, region = ASIA
prefix source = geographic
```

This display shows the following information.

TABLE 14 GSLB policy information

This field...	Displays...
prefix length	Specifies the length of the address prefix. The GSLB ServerIron ADX initially generates the prefix tree using the IANA (geographic) allocated address prefixes, which have variable lengths. Dynamically generated cache entries (generated by client queries) have a fixed prefix length, as defined by the RTT cache-length parameter. The default is 20.
prefix	Specifies the prefix. All client addresses beginning with this prefix are aggregated in a single RTT entry.
region	Specifies the geographic location of this client prefix. This field can have one of the following values: • ASIA • EUROPE • N-AM: North America • S-AM: South America
prefix source	Specifies the prefix source. This field can have one of the following values: • geographic: displayed for static entries (entries generated by the GSLB ServerIron ADX itself when initializing the RTT cache) • client query: displayed for entries generated by client queries • static: displayed for static entries entered by you (refer to "Adding static prefix cache entries" on page 55) **NOTE:** If a static entry is long enough (greater than 20 bits) and has been accessed by a client query, the entry can show both sources. Notice that a prefix cache entry can have more than one source.
site	Specifies the name of the site.
ServerIron ADX	Specifies the name and IP address of the ServerIron ADX.
rtt	Specifies the RTT value.

Displaying GSLB resources

For GSLB parameters, you can display the number of currently configured items and the maximum number of items you can configure on the ServerIron ADX. To display this information, use the following CLI method.

To display GSLB resource information, enter the following command at any level of the CLI.

```
ServerIronADX# show gslb resources
GSLB resource usage:
                    Current   Maximum
sites               1         128
ServerIronADXs         0         200
ServerIronADXs' VIPs   0         2048
dns zones           0         256
dns hosts           0         600
health-checks app.  0         600
dns IP addrs.       0         2048
affinities          0         128
static prefixes     0         250
user geo prefixes   0         64
prefix cache        108       10128
RTT entries         0         10000
GSLB host policies  0         100
```

The values in the Current column indicate how many of each GSLB configuration or data item are currently on the GSLB ServerIron ADX. The values in the Maximum column list the maximum number of each item the GSLB ServerIron ADX can hold.

Syntax: **show gslb resources**

This command shows the following information.

TABLE 15 GSLB resources

This field...	Displays...
sites	The number of remote sites configured on the GSLB ServerIron ADX.
ServerIron ADXs	The number of remote site ServerIron ADXs configured on the GSLB ServerIron ADX. Each remote site ServerIron ADXs is associated with a site. When you add a remote site ServerIron ADX, the GSLB ServerIron ADX uses the GSLB protocol to establish a TCP session with port 182 on the remote ServerIron ADX, for gathering information to use with the GSLB policy.
ServerIron ADXs’ VIPs	The number of virtual IP addresses (VIPs) configured on the site ServerIron ADXs that the GSLB ServerIron ADX has cached, and the maximum number of site VIPs the GSLB ServerIron ADX can cache.
dns zones	The number of zone names currently configured on this GSLB ServerIron ADX and the maximum number that can be configured.
dns hosts	The number of host names currently configured on this GSLB ServerIron ADX and the maximum number that can be configured.
health-checks app.	The number of applications currently configured on this GSLB ServerIron ADX and the maximum number that can be configured. The ServerIron ADX performs Layer 4 and, if applicable, Layer 7 health checks on each application.

TABLE 15 GSLB resources (Continued)

This field...	Displays...
dns IP addrs.	The number of IP addresses the GSLB ServerIron ADX has learned from the DNS server, and the maximum number of DNS records the GSLB ServerIron ADX can store in memory.
affinities	The number of affinity definitions currently configured on the GSLB ServerIron ADX and the maximum number that can be configured.
static prefixes	The number of statically configured prefixes in the GSLB ServerIron ADX's prefix cache, and the maximum number or statically configured prefixes the cache can hold. For information, refer to "Adding static prefix cache entries" on page 55.
prefix cache	The total number of prefixes currently in the prefix cache, and the maximum number the cache can hold. The prefix entries include static ones used for geographic information, user-configured prefixes, and dynamic prefixes created when client queries are received. Dynamic entries age out when unused.
RTT entries	The number of cached per-prefix, per-domain name RTT records. For each client prefix, the GSLB ServerIron ADX stores the most recently accessed domain names (up to 10 per client, ordered from most to least recent). For each domain name the GSLB ServerIron ADX stores the site the GSLB ServerIron ADXs that currently have the best RTT to the client prefix (up to four such the GSLB ServerIron ADXs: two current best choices plus two potentials). The GSLB ServerIron ADX has separate records for each domain name because the closest site can be different for different domain names (unless every remote ServerIron ADX serves every domain name). If the maximum is reached, the GSLB ServerIron ADX stops creating new records.

Displaying dynamic server information

When you configure GSLB, the ServerIron ADX creates dynamic real server configurations based on the IP addresses the GSLB ServerIron ADX receives in response to DNS queries sent to the real DNS server. These real servers are created for health check purposes only, and do not play a role in SLB. In the dynamic configurations, the site IP addresses contained in DNS replies are the names and IP addresses of the real servers. The ServerIron ADX creates internal virtual servers and then binds the dynamic real servers to the virtual servers based on the application ports you specify when you add GSLB zones and hosts.

This information can be useful when troubleshooting your GSLB configuration, by showing you the internal servers and port bindings the ServerIron ADX created based on your GSLB configuration. For example, if your configuration uses multiple zone names associated with the same IP address, you can verify that the ServerIron ADX created an alias TCP port number for each additional zone and application associated with the IP address.

The commands and displays for dynamic server configuration information are based on the commands and displays for SLB server configuration information. You can display the following dynamic configuration information:

- **Real server information:** There is one dynamically created real server per IP address.
- **Virtual server information:** There is one dynamically created virtual server per domain name.
- **Port binding information:** The TCP and UDP ports
- **Session statistics:** Another way to list the real servers.

To display dynamic server information, enter the commands shown in the following examples. The portions of the output that are shown in bold type are those of interest.

Displaying dynamic real server information

To display the real servers that the ServerIron ADX dynamically has created for the site addresses from DNS replies, enter the following information.

```
ServerIronADX(config)# show server dynamic real
Real Servers Info
Name : 209.157.22.229
IP:209.157.22.229  Range:1    State:Active          Wt:1     Max-conn:1000000
Port    State    Ms CurConn TotConn Rx-pkts  Tx-pkts  Rx-octet   Tx-octet   Reas
----    -----    -- ------- ------- -------  -------  --------   --------   ----
http    active   0  0       0       0        0        0          0          0
default unbnd    0  0       0       0        0        0          0          0
Server  Total       0       0       0        0        0          0          0
Name : 209.157.22.230
IP:209.157.22.130  Range:1    State:Active          Wt:1     Max-conn:1000000
Port    State    Ms CurConn TotConn Rx-pkts  Tx-pkts  Rx-octet   Tx-octet   Reas
----    -----    -- ------- ------- -------  -------  --------   --------   ----
http      failed   0  0       0       0        0        0          0          0
default unbnd    0  0       0       0        0        0          0          0
Server  Total       0       0       0        0        0          0          0
```

This example shows real servers dynamically created for two sites that were listed in DNS replies.

Syntax: show server dynamic real

Displaying virtual server information

You can display internal virtual servers. The purpose of these servers is to allow the ServerIron ADX to bind to the dynamically created real servers. The ServerIron ADX uses private IP addresses starting with 10.10.10.10 for the names and IP addresses of the virtual servers. The ServerIron ADX does not respond to pings or ARP requests to the addresses it uses for the internal virtual servers. Thus, if your network also uses these addresses, the virtual servers do not create address conflicts.

NOTE
Since the dynamic virtual servers use addresses in the 10.10.10.x/23 subnet for the internal database, a GSLB ServerIron ADX cannot support user-configured real and virtual servers in this address range.

```
ServerIronADX(config)# show server dynamic virtual
```

```
Virtual Servers Info
Server Name: 10.10.10.10     IP : 10.10.10.10     :   1
Status: enabled  Predictor: round-robin  TotConn: 0
Dynamic: Yes    HTTP redirect: disabled
ACL: id =   0
Sym: group =  1 state =  5 priority =   0 keep =   0
 Activates =    1, Inactive= 0
Port    State     Sticky  Concur  Proxy      CurConn   TotConn   PeakConn
http    enabled   NO      NO      NO               0         0          0
default enabled   NO      NO      NO               0         0          0
Server Name: 10.10.10.11     IP : 10.10.10.11     :   1
Status: enabled  Predictor: round-robin  TotConn: 0
Dynamic: Yes    HTTP redirect: disabled
ACL: id =   0
Sym: group =  1 state =  5 priority =   0 keep =   0
 Activates =    1, Inactive= 0
Port    State     Sticky  Concur  Proxy      CurConn   TotConn   PeakConn
70      enabled   NO      NO      NO               0         0          0
default enabled   NO      NO      NO               0         0          0
```

Syntax: show server dynamic virtual

Displaying the port bindings

To display the port bindings the ServerIron ADX creates for the dynamically created real servers and virtual servers, enter the following command.

```
ServerIronADX(config)# show server dynamic bind
Virtual Server Name: 10.10.10.10,   IP: 10.10.10.10
        http -------> 209.157.22.229: 209.157.22.229,  http (remote)
Virtual Server Name: 10.10.10.11,   IP: 10.10.10.11
          70 -------> 209.157.22.230: 209.157.22.230,  70 (remote)
```

This example shows that the ServerIron ADX has bound internal virtual server 10.10.10.10 to real server 209.157.22.229 for TCP port 80 (HTTP). The ServerIron ADX also has bound internal virtual server 10.10.10.11 to real server 209.157.22.230, using TCP port 80.

Syntax: show server dynamic bind

The **show server dynamic bind** command shows the port bindings the ServerIron ADX creates for the dynamically created real servers and virtual servers.

Listing the real servers

To list the real servers, enter the following command.

```
ServerIronADX(config)# show server dynamic sessions
Avail. Sessions      =     524287  Total Sessions       =     524288
Total C->S Conn      =         90  Total S->C Conn      =          0
Total Reassign       =          0  Unsuccessful Conn    =          2
Server State - 1:enabled, 2:failed, 3:test, 4:suspect, 5:grace_dn, 6:active
Real Server     State   CurrConn    TotConn TotRevConn   CurrSess   PeakConn
209.157.22.229      6          0          0          0          0          0
209.157.22.230      6          0          0          0          0          0
```

Syntax: show server dynamic sessions

The **show server dynamic** sessions command provides a simple way to list the real servers. The output is based on the output for the **show server sessions** command. However, in the case of dynamically created servers, there are no meaningful session statistics in this display.

Specifying the source IP of probes

In previous GSLB implementations, both the ICMP and DNS RTT probes sent out for the active RTT gathering feature used the IP address of the outgoing interface to the LDNS server as the source IP.

Starting in 09.2.00, you can specify the IP address to be used as the source IP of these probes, by using the following command.

Syntax: **gslb src-ip-active-rtt** <*ip-address*>

The <*ip-address*> is an IP address already configured on a ServerIron ADX interface.

If you specify an IP address not configured on the device, the previous CLI command will reject it. Additionally if you remove the IP address on an interface (and this is the IP configured for active RTT probing), then the ServerIron ADX will remove this IP as the GSLB source IP for active RTT gathering.

Displaying information in the prefix cache

The GSLB ServerIron ADX's prefix cache stores information received from site ServerIron ADXs through the GSLB protocol. You can display information in the prefix cache using the **show gslb cache** command.

To display all entries in the GSLB ServerIron ADX's prefix cache, enter the following command.

```
ServerIronADX# show gslb cache all
prefix length = 8, prefix = 3.0.0.0, region = N-AM
prefix source = geographic (static),

prefix length = 8, prefix = 4.0.0.0, region = N-AM
prefix source = geographic (static),

prefix length = 8, prefix = 6.0.0.0, region = N-AM
prefix source = geographic (static),
...
```

Syntax: **show gslb cache all**

To display all the static entries in the GSLB ServerIron ADX's prefix cache, enter the following command.

```
ServerIronADX# show gslb cache all static
prefix length = 24, prefix = 192.168.20.0, region = N-AM
prefix source = static,

prefix length = 29, prefix = 192.168.20.248, region = N-AM
prefix source = static,
...
```

Syntax: **show gslb cache all static**

To display the affinity entries configured for client prefixes on the GSLB ServerIron ADX, enter the following command.

```
ServerIronADX# show gslb cache all affinity
prefix length = 24, prefix = 28.1.1.0, region = N-AM
prefix source = affinity,
affinity = site: local, ServerIronADX: 1.1.1.102
```

Syntax: **show gslb cache all affinity**

To display the statically generated geographic cache entries on the GSLB ServerIron ADX, enter the following command.

```
ServerIronADX# show gslb cache all geographic static
prefix length = 8, prefix = 3.0.0.0, region = N-AM
prefix source = geographic (static),

prefix length = 8, prefix = 4.0.0.0, region = N-AM
prefix source = geographic (static),
...
```

Syntax: **show gslb cache all geographic static**

To display the user-configured geographic cache entries on the GSLB ServerIron ADX, enter the following command.

```
ServerIronADX# show gslb cache all geographic user-configured
prefix length = 20, prefix = 1.1.0.0, region = ASIA
prefix source = geographic (user-configured), rtt-update,

  site = local,  ServerIronADX = (1.1.1.102),  rtt = 7 (x100 usec)

prefix length = 24, prefix = 10.10.10.0, region = ASIA
prefix source = geographic (user-configured),
```

Syntax: **show gslb cache all geographic user-configured**

To display cache entries that contain RTT information reported by a specified Site ServerIron ADX, enter a command such as the following:

```
ServerIronADX# show gslb cache all 1.1.1.102
  prefix = 1.1.0.0, prefix length = 20
    site = local,  ServerIronADX = (1.1.1.102),  rtt = 7 (x100 usec)
```

Syntax: **show gslb cache all** <*ip-addr*>

The <*ip-addr*> is the address of a Site ServerIron ADX.

To display the cache entries for a specified prefix longer than a specified length, enter a command such as the following:

```
ServerIronADX# show gslb cache 2.1.1.1 longer-than 8
prefix length = 24, prefix = 2.1.1.0, region = N-AM
prefix source = static,
```

Syntax: **show gslb cache** <*ip-addr*> **longer-than** <*prefix-length*>

The example above displays all prefix cache entries for address 2.1.1.1, with a prefix length from 8 to 31. You can specify a <*prefix-length*> from 1-31.

To display the cache entries for a specified prefix shorter than a specified length, enter a command such as the following:

```
ServerIronADX# show gslb cache 1.1.0.0 smaller-than 24
prefix length = 20, prefix = 1.1.0.0, region = ASIA
prefix source = geographic (user-configured), rtt-update,

site = local,  ServerIronADX = (1.1.1.102),  rtt = 7 (x100 usec)
```

Syntax: **show gslb cache** <*ip-addr*> **smaller-than** <*prefix-length*>

The example above displays all prefix cache entries for address 1.1.0.0, with a prefix length from 1 to 24.

To display the cache entries for a specified prefix with a length in a specified range, enter a command such as the following:

```
ServerIronADX# show gslb cache 1.1.1.1 range 2 29
prefix length = 20, prefix = 1.1.0.0, region = ASIA
prefix source = geographic (user-configured), rtt-update,

  site = local,  ServerIronADX = (1.1.1.102),  rtt = 7 (x100 usec)

prefix length = 24, prefix = 1.1.1.0, region = ASIA
prefix source = static,
```

Syntax: **show gslb cache** <*ip-addr*> **range** <*length-lower*> <*length-upper*>

The example above displays all prefix cache entries for address 1.1.0.0, with a prefix length from 2 to 29.

SNMP traps and syslog messages

The ServerIron ADX software can generate the following SNMP traps and syslog messages related to GSLB. All traps and syslog messages are enabled by default.

- GSLB ServerIron ADX events:
  - Establishment of the GSLB protocol connection between the GSLB ServerIron ADX and the remote ServerIron ADX
  - Termination of the GSLB protocol connection between the GSLB ServerIron ADX and the remote ServerIron ADX
- Remote site ServerIron ADX events:
  - Establishment of the GSLB protocol connection between the remote ServerIron ADX and the GSLB ServerIron ADX
  - Termination of the GSLB protocol connection between the remote ServerIron ADX and the GSLB ServerIron ADX
- Health-check events:
  - The GSLB ServerIron ADX determines that the IP address for a domain name is active
  - The GSLB ServerIron ADX determines that the IP address for a domain name is down
  - A TCP or UDP port passes the Layer 4 health check and its status changes to "active"
  - A TCP or UDP port fails the Layer 4 health check and its status changes to "down"

NOTE
All the health check events are on the GSLB ServerIron ADX, not on the remote site ServerIron ADXs.

A given domain name can be associated with multiple health check TCP or UDP ports. In that case, the GSLB ServerIron ADX considers an IP address to be active only if all its associated TCP and UDP ports pass their health checks.

State transitions of individual ports are determined as a part of the health check procedure. However, state transitions for IP addresses are detected during GSLB decision making (when the GSLB ServerIron ADX is processing a DNS response or when you display zone information). In these cases, health check status changes affect the GSLB decisions.

Syslog messages

By default, the ServerIron ADX's syslog buffer is enabled and contains up to 50 entries. To display the GSLB and other syslog messages, enter the following command at any level of the CLI.

```
ServerIronADX> show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Buffer logging: level ACDMEINW, 16 messages logged
    level code: A=alert C=critical D=debugging M=emergency E=error
                I=informational N=notification W=warning
Dynamic Log Buffer (50 entries):
00d00h01m28s:N:L4 gslb health-check 209.157.22.210 of brocade.com status changed
to up
00d00h01m28s:N:L4 gslb health-check 209.157.22.209 of brocade.com status changed
to up
00d00h01m01s:I:Interface ethernet16, state up
00d00h01m01s:I:Interface ethernet2, state up
00d00h00m34s:N:L4 gslb health-check 209.157.22.210 of brocade.com port 80 is up
00d00h00m32s:N:L4 gslb health-check 209.157.22.209 of brocade.com port 80 is up
00d00h00m32s:N:L4 server 209.157.23.59 kandrew TCP port 80 is up
00d00h00m32s:N:L4 server 209.157.23.59 kandrew is up
00d00h00m31s:N:L4 gslb connection to site sunnyvale ServerIronADX 209.157.22.210
slb-2 is up
00d00h00m31s:N:L4 gslb connection to site sunnyvale ServerIronADX 209.157.22.209
slb-1 is up
00d00h00m31s:I:Bridge topology change, vlan 1, interface 16, changed state to
forwarding
00d00h00m07s:N:L4 server 209.157.23.130 dns-ivy TCP port 53 is up
00d00h00m07s:N:L4 server 209.157.23.130 dns-ivy is up
00d00h00m06s:I:Bridge topology change, vlan 1, interface 2, changed state to
forwarding
00d00h00m03s:I:Bridge root changed, vlan 1, new root ID 800000e0520002d1, root
interface 16
00d00h00m00s:I:Warm start
```

Syntax: show logging

In this example, the GSLB messages are shown in bold type. The GSLB messages in this example all apply to the ServerIron ADXs at the Sunnyvale site. Three types of messages are shown:

- The first two GSLB messages are shown nearest the bottom, since new messages appear at the top. These two messages indicate that the GSLB ServerIron ADX has established a GSLB protocol connection to the site ServerIron ADXs (slb-1 at 209.157.22.209 and slb-2 at 209.157.22.210).
- The next two GSLB messages indicate that the Layer 4 health checks for TCP port 80 were completed successfully. For sites with other applications, the ServerIron ADX sends separate Layer 4 TCP or UDP health checks for each of those applications.

- The final two GSLB messages in this example (the ones nearest the top of the log) indicate that the site ServerIron ADXs responded to the Layer 3 health check (IP ping).

Disabling and re-enabling traps

All traps, including GSLB traps, are enabled by default.

To disable a GSLB trap, enter a command such as the following:

```
ServerIronADX(config)# no snmp-server enable traps l4-gslb-remote-si-down
```

The command in this example disables the trap that occurs if a remote site ServerIron ADX fails its Layer 3 health check and its status therefore changes from “up” to “down”.

Syntax: [no] snmp-server enable traps <*trap-type*>

For GSLB, the trap type can be one of the following:

- l4-gslb-remote-gslb-si-down: Generated when the GSLB protocol connection from this site ServerIron ADX to a remote GSLB ServerIron ADX goes down.
- l4-gslb-remote-gslb-si-up: Generated when the GSLB protocol connection from this site ServerIron ADX to a remote GSLB ServerIron ADX comes up.
- l4-gslb-remote-si-down: Generated when the GSLB protocol connection from this GSLB ServerIron ADX to a remote site ServerIron ADX goes down.
- l4-gslb-remote-si-up: Generated when the GSLB protocol connection from this GSLB ServerIron ADX to a remote site ServerIron ADX comes up.
- l4-gslb-health-check-ip-down: Generated when GSLB determines that the IP address belonging to a domain name for which the ServerIron ADX is providing GSLB is down.
- l4-gslb-health-check-ip-up: Generated when GSLB determines that the IP address belonging to a domain name for which the ServerIron ADX is providing GSLB is now active.
- l4-gslb-health-check-ip-port-down: Generated when an application port in a domain on the site IP address fails its Layer 4 TCP or UDP health check, resulting in a status change to “down”.
- l4-gslb-health-check-ip-port-up: Generated when an application port in a domain on the site IP address passes its Layer 4 TCP or UDP health check, resulting in a status change to “up”.

GSLB error handling for unsupported DNS requests

The ServerIron ADX can perform GSLB on client queries for the following DNS record types:

- IPv4 address records (A records)
- Canonical Name records (CNAME records)

In many GSLB topologies, the GSLB ServerIron ADX front-ends a DNS server. When the GSLB ServerIron ADX receives a client query for supported DNS record types, the GSLB ServerIron ADX forwards the client query to the DNS server. In turn, the DNS server sends a response to the GSLB ServerIron ADX, which performs GSLB on the response, then forwards the response to the client.

Similarly, when the GSLB ServerIron ADX receives a client query for unsupported DNS record types, such as IPv6 address records (AAAA records), Name Server records (NS records), or Mail Exchange records (MX records), the GSLB ServerIron ADX forwards the client query to the DNS server. The DNS server sends a response to the GSLB ServerIron ADX, which then forwards the response, unaltered, to the client.

This process works in topologies where the GSLB ServerIron ADX front-ends a DNS server. However, not all GSLB topologies require a DNS server. For example, when the GSLB ServerIron ADX is configured as a DNS cache proxy with DNS override and IP lists. In this case, when the GSLB ServerIron ADX receives a client query for an unsupported DNS record type, the GSLB ServerIron ADX cannot forward the client request to a DNS server, so it drops the query without sending a response to the client, subsequently causing the client to time out.

GSLB error handling enables the GSLB ServerIron ADX to send error messages in response to client requests for unsupported DNS record types. When clients receive these error messages from the GSLB ServerIron ADX, the clients query for another DNS record type instead of continuing to query for the unsupported record type, or timing out on the query altogether.

GSLB ServerIron ADX intercepts queries for unsupported DNS record types, parses them, and checks if there is a DNS server available to send the query to. If so, it forwards the request to that DNS server and sends the response, unaltered, to the client. If the GSLB ServerIron ADX determines that no DNS server is available to process the request, it generates a response with the appropriate error code and sends it to the client. The response prevents the client from timing out.

Note that in GSLB topologies that require a DNS server, requests for unsupported DNS record types are always handled by the DNS server, and not by the GSLB ServerIron ADX.

Default settings for GSLB error handling

The configuration default for GSLB error handling differs depending on your GSLB configuration:

- If the GSLB ServerIron ADX is a plain DNS proxy, GSLB error handling is not supported. This is because a DNS server is always required for this configuration, and client requests always go to the DNS server.
- If the GSLB ServerIron ADX is a cache proxy, GSLB error handling is enabled by default.
- If the GSLB ServerIron ADX is configured for transparent Intercept mode, GSLB error handling is disabled by default. If necessary, you can enable error handling (refer to "Disable or re-enabling GSLB error handling" on page 190).

Using GSLB error handling with transparent intercept mode

In the transparent intercept mode, GSLB error handling is disabled by default.

Enabling error handling with transparent intercept mode can be effective in certain configurations. For example, when the GSLB ServerIron ADX is configured to intercept and directly respond to requests for *www.gslb.com*, and the DNS server that it is intercepting has no record types other than A records for *www.gslb.com*. In this example, the GSLB ServerIron ADX responds to client queries for MX records for *www.gslb.com*, as follows:

- With error handling enabled, the GSLB ServerIron ADX directly responds with an error handling message. Since the DNS server does not have any MX records, it would not be efficient if the GSLB ServerIron ADX forwarded the query to the DNS server. Thus, configuring the GSLB ServerIron ADX to directly conduct error handling reduces the latency for the response to that client.
- With error handling disabled, the GSLB ServerIron ADX forwards the query to the DNS server, which responds with an error handling reply. Without error handling, latency is increased in the response time to the client.

Error handling response format

The GSLB error handling response format complies with RFC 2308, NODATA type 3 response. By default, the return code (rcode) is **noerror**. The RFC 2308 format is as follows.

```
NO DATA RESPONSE:  TYPE 3
Header:
   RDCODE=NOERROR
Query:
   ANOTHER.EXAMPLE.A
Answer:
   <empty>
Authority:
   <empty>
Additional:
   <empty>
```

The above is an authoritative answer with rcode=NOERROR, answer=0, and no Start of Authority (SOA) record. This error handling response prevents the client from timing out on the query and causes the client to query for another record type instead of continuing to query for the unsupported record type.

Although Brocade does not advise you to do so, you can configure the return code for error handling responses. Refer to the section "Configuring the return code" on page 190.

Disable or re-enabling GSLB error handling

GSLB error handling is enabled by default in cache proxy configurations. It is disabled by default in transparent intercept mode.

To disable GSLB error handling, enter the following command.

```
GSLB-ServerIronADX(config)# gslb no-error-handling
```

Syntax: [no] gslb no-error-handling

To re-enable GSLB error handling, enter the following command.

```
GSLB-ServerIronADX(config)#no gslb no-error-handling
```

Configuring the return code

Although Brocade does not advise you to do so, you can configure the return code for error handling responses, by entering a command such as the following:

```
GSLB-ServerIronADX(config)# gslb dns-rcode notimp
```

This option causes the GSLB ServerIron ADX to respond with the error code **notimp** (not implemented) in the error handling response.

Syntax: [no] gslb dns-rcode [former | noerror | notimp | nxdomain | refused | servfail]

former = format error

noerror = no error (the default)

notimp = not implemented

nxdomain = non-existant domain

refused = query refused

servfail = server failure

NOTE
Do not change the error code unless you are absolutely certain of the effect of the configuration. For example, if you configure nxdomain as the return code, the GSLB ServerIron ADX responds to an unsupported query type with this error code. When the client receives the nxdomain response, the client typically stops attempting to resolve any other record type for that name. For example, an nxdomain response to an IPv6 record type might stop the client from sending a query for an IPv4 record type, even though IPv4 record types exist for that domain. Furthermore, if this response (with nxdomain rcode) is negatively cached, it can result in a potential denial-of-service attack for a particular domain name.

Viewing error handling statistics

You can view the number of client requests for unsupported DNS record types for which the GSLB ServerIron ADX generated an error handling response. Enter the following command at any level of the CLI.

```
ServerIronADX(config)# show gslb global-stat

DNS cache proxy stat:

Direct response      =          1


DNS query intercept stat:

Redirect             =          0  Direct response      =          0


Unsupported query types stat:

Error handling cnt   =          3
```

In the example above, the **Error handling cnt** shows that the GSLB ServerIron ADX generated and sent error handling responses for three client queries.

Syntax: **show gslb global-stat**

Clearing the error handling statistics

To clear the error handling statistics for the GSLB ServerIron ADX, enter the following command.

```
GSLB-ServerIronADX# clear gslb unsupported-response-cnt
```

Syntax: **clear gslb unsupported-response-cnt**

To confirm the statistics were cleared, use the **show gslb global-stat** command.

Chapter

Global Server Load Balancing for IPv6

2

Global server load balancing for IPv6 overview

Global Server Load Balancing (GSLB) enables a ServerIron ADX to add intelligence to authoritative Domain Name System (ADNS) servers by serving as a proxy to these servers and providing optimal IP addresses to the querying clients. As a DNS proxy, the GSLB ServerIron ADX evaluates the IP addresses in the DNS replies from the ADNS and places the “best” host address for the client at the top of the DNS response. The GSLB ServerIron ADX can also directly respond to the DNS queries in the DNS cache proxy with DNS override mode.

As data centers increasingly move towards migrating some or all of their servers and services to IPv6, there is an increasing need to perform GSLB for these IPv6 entities in addition to IPv4. Brocade GSLB ServerIron ADX performs GSLB for both IPv4 (A records) and IPv6 (AAAA records) and directs the clients to the optimal IP address based on the configured GSLB policies.

In the current implementation, the ServerIron ADX supports global server load balancing and redundancy for IPv6 addresses in DNS cache proxy with DNS override mode only. In this mode, the IPv6 addresses for hosts are configured on the ServerIron ADX GSLB controller, which acts as the authoritative DNS server for the configured zones. The GSLB controller does not have a backend DNS server. Instead, the GSLB controller intercepts DNS queries and generates the DNS response by applying GSLB policies on the IPv6 list configured for the hostname.

The GSLB controller ensures that a client always receives a DNS reply for a host site that is the best choice among the available hosts. Just as with data centers in which the content for a domain can be serviced by IPv4 and IPv6 servers, a domain on the GSLB ServerIron ADX can have a mix of IPv4 and IPv6 domain IPs. If the client makes an A record query, then the best IPv4 domain IP will be selected for the client. Similarly, if the client makes a AAAA query, then the best IPv6 domain IP will be selected for that client.

ServerIron ADX GSLB for IPv6 configuration tasks are covered in four sections within this chapter:

- Basic GSLB for IPv6 configuration: Basic configuration tasks include the configuration of the GSLB ServerIron ADX and the site ServerIron ADXs to support GSLB of IPv6 addresses. This includes the configuration of a virtual IP address (VIP) for the ADNS, the configuration of DNS cache proxy mode with override lists, and the definition of zones and sites on the GSLB ServerIron ADX. The GSLB protocol must be enabled on the site ServerIron ADX.
- Advanced GSLB for IPv6 configuration: Advanced configuration tasks include the configuration of GSLB policies and diyr persistence for IPv6 addresses.
- Displaying GSLB for IPv6 configurations: This section describes commands for viewing GSLB configurations on the ServerIron ADX.
- Troubleshooting GSLB for IPv6 configurations: This section describes steps that may be taken to troubleshoot GSLB for IPv6 configurations.

GSLB for IPv6 feature support

In the initial release of GSLB for IPv6, a subset of modes, GSLB policy metrics, and other features and modules are supported.

Modes

In the current implementation, GSLB ServerIron ADX performs GSLB for IPv6 domain IP addresses only in the DNS cache proxy with Override mode.

The following modes are not supported:

- Proxy for DNS server
- DNS cache proxy only
- Transparent DNS query intercept
- Override only

Policy metrics

GSLB ServerIron ADX does not currently support the following policy metrics for load balancing IPv6 addresses:

- Active and passive round-trip time
- Connection load

For information about policy metrics supported with GSLB for IPv6, see "Configuring GSLB policy metrics for IPv6" on page 204.

Features

GSLB ServerIron ADX for IPv6 does not currently support the following modules and features:

- Affinity
- GSLB affinity for high availability
- GSLB domain-level affinity
- TCP DNS
- Private VIPs for GSLB

Secure GSLB

Secure GSLB is not supported with GSLB for IPv6.

Fragmentation

Fragmentation is not supported in this initial release. Customers should either configure an active-only policy or best-only policy (see "Configuring DNS response parameters" on page 229) or ensure that the number of IP addresses configured in the IP list is small enough to avoid fragmentation (i.e., assuming a full length query name (255 bytes)):

- If the client does not advertise EDNS0 header with a buffer larger than 512 bytes, eight IPv6 addresses per host are supported in the response.
- If the client advertises EDNS0 header with a buffer smaller than 512 bytes, forty IPv6 addresses per host are supported in the response.

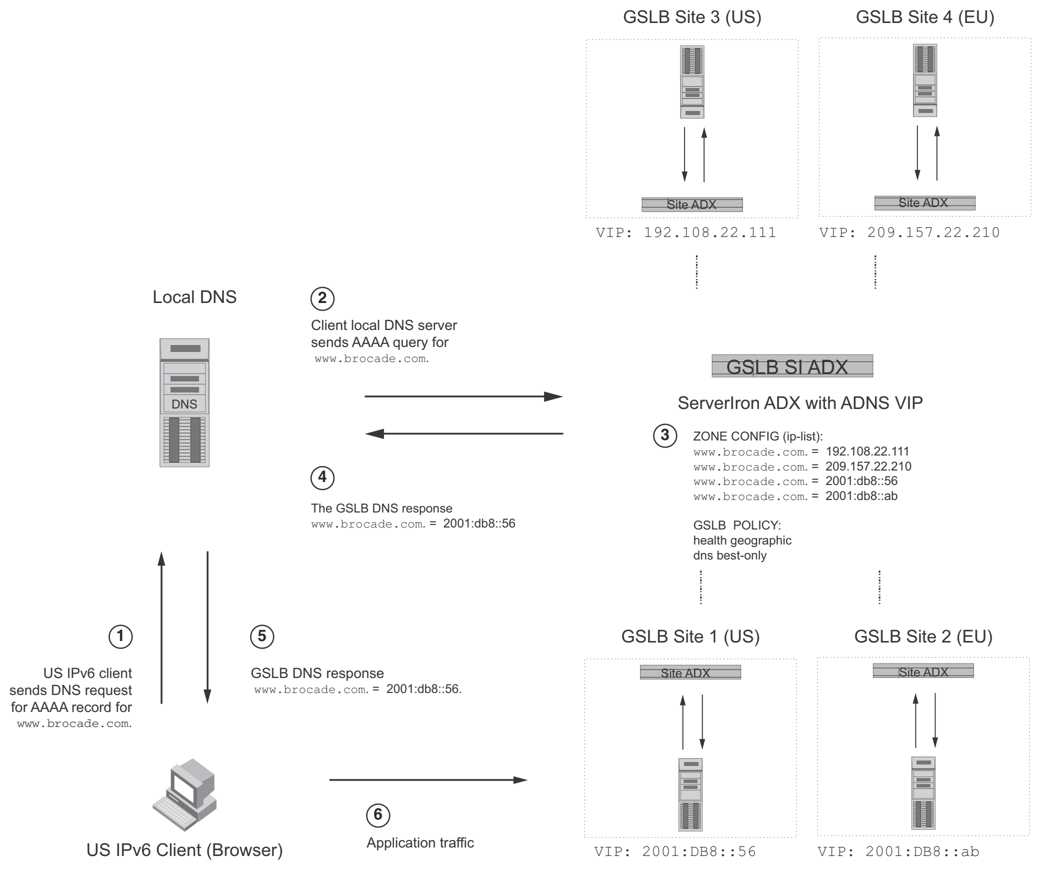
GSLB for IPv6 example

Typically, GSLB for IPv6 is used to distribute IPv6 traffic to multiple sites for load balancing, geographic proximity, or redundancy.

Figure 12 shows a deployment of IPv6 GSLB in DNS cache proxy with DNS override mode. The GSLB controller acts as the authoritative DNS server for the www.brocade.com domain. The domain IPs for www.brocade.com are a mix of IPv4 and IPv6 addresses. When the GSLB controller receives DNS queries from resolvers (local DNS), it generates a response based on a configured GSLB policy.

In this example, the GSLB controller sees that the client is geographically closer to the US site and, therefore, directs application traffic to the closer VIP.

FIGURE 12 IPv6 GSLB configuration


GSLB Site 3 (US)
GSLB Site 4 (EU)
Site ADX
Site ADX
VIP: 192.108.22.111
VIP: 209.157.22.210
Local DNS
DNS
2
Client local DNS server sends AAAA query for www.brocade.com.
GSLB SI ADX
ServerIron ADX with ADNS VIP
3
ZONE CONFIG (ip-list):
www.brocade.com. = 192.108.22.111
www.brocade.com. = 209.157.22.210
www.brocade.com. = 2001:db8::56
www.brocade.com. = 2001:db8::ab
GSLB POLICY:
health geographic
dns best-only
4
The GSLB DNS response
www.brocade.com. = 2001:db8::56
1
US IPv6 client sends DNS request for AAAA record for www.brocade.com.
5
GSLB DNS response
www.brocade.com. = 2001:db8::56.
GSLB Site 1 (US)
GSLB Site 2 (EU)
Site ADX
Site ADX
6
Application traffic
US IPv6 Client (Browser)
VIP: 2001:DB8::56
VIP: 2001:DB8::ab

The GSLB controller makes decisions based on the GSLB policy. In the example above, both the IPv6 VIPs were healthy, so client was directed to the IPv6 VIP that was geographically closer based on the configured policy. If the VIP at the geographically closer site (the US site) was down, the GSLB controller would direct traffic to the EU site.

1. US IPv6 client (browser) sends a DNS request for the website brocade.com.
2. The client's local DNS server sends a recursive query for www.brocade.com to the GSLB controller (a ServerIron ADX with ADNS VIP).
3. The GSLB controller determines that the request is for an IPv6 address (query type AAAA) and so checks the IPv6 address list and identifies GSLB Site 1 (US) as the optimal IP for clients in the US based on the configured GSLB policy. (Similarly, a request for an IPv4 address would have been directed to GSLB Site 3 or Site 4.)
4. The GSLB controller sends a GSLB DNS response with the VIP address (2001:DB8::56) to the local DNS server. Note that the controller only sends the best IP to the querying client because "dns best-only" is configured in the GSLB policy. In the absence of this configuration, the GSLB controller would have sent back both IPv6 addresses with the best IP (2011:DB8::56) at the top of the response.
5. The local DNS server sends the GSLB DNS response to the querying client.
6. The US IPv6 client initiates communication with the selected VIP. Application traffic flows directly between the IPv6 client and the IPv6 VIP at GSLB Site 1.

Basic GSLB for IPv6 configuration

Basic configuration tasks include the configuration of the GSLB ServerIron ADX and the site ServerIron ADXs to support GSLB of IPv6 addresses. Tasks include the configuration of a VIP for the ADNS, the enabling and configuration of DNS cache proxy mode with override lists, and the definition of zones and sites on the GSLB ServerIron ADX. Also, the GSLB protocol must be enabled on the site ServerIron ADXs.

The features shown in Table 16 describe the configuration parameters required for a basic GSLB for IPv6 configuration.

TABLE 16 Basic GSLB for IPv6 configuration tasks

Feature	See page...
On GSLB ServerIron ADX controller	
Adding a VIP for the ADNS server	page 197
Enabling DNS cache proxy	page 197
Enabling DNS override	page 198
Specifying the zones and the host names within the zones	page 198
Specifying DNS override IP lists	page 199
Specifying the sites and the ServerIron ADXs within the sites	page 200
On Site ServerIron ADXs	
Enabling the GSLB protocol	page 201

Configuring the GSLB controller

The GSLB ServerIron ADX supports global server load balancing in DNS cache proxy with DNS override mode. In this mode, the GSLB controller responds directly to DNS queries with the “best” address, from a configured list of addresses, at the top of the DNS response.

When you enable the DNS override feature, you need to configure an IP list for the required domains. The ServerIron ADX performs health checks on the IP addresses configured for the domains and directly responds to client queries by using the GSLB policy to select the best IP address from the IP list configured for the requested domain.

NOTE
Although you do not need a real DNS server when you combine DNS cache proxy with DNS override, you still need to configure a virtual IP address for the DNS server. Clients send queries to the virtual IP address.

Adding a VIP for the ADNS server

The **server virtual-name-or-ip** command enables you to define a virtual server port on the GSLB ServerIron ADX. The virtual server acts as the authoritative DNS server (ADNS) for a domain. Clients send queries to the virtual IP address.

The ADNS VIP intercepts DNS requests for the domains configured on it. If the query is of type AAAA, then it performs global server load balancing in accordance with the configured GSLB policy on all IPv6 domain IP addresses for the requested domain and places the best IPv6 address at the top of the response.The ADNS VIP can be either an IPv4 or an IPv6 address.

To define an IPv6 intercept VIP on the GSLB ServerIron ADX, enter commands such as the following:

```
ServerIronADX(config)# server virtual-name-or-ip dns6-vip 2001:DB8::200
ServerIronADX(config-vs-dns-proxy)# port dns
```

The command in this example adds a virtual server called “dns6-vip” with the IP address 2001:DB8::200. The GSLB ServerIron ADX processes all client queries sent to this address. This command changes the CLI to the Virtual Server configuration level. At this level, the **port dns** command adds the DNS port to the virtual server.

Syntax: **[no] server virtual-name-or-ip** <*name*> [<*ipv4-address*> | <*ipv6-address*]

The <*name*> parameter specifies the name for for the virutal server. The <*ipv4-address*> and <*ipv6-address*> parameters specify the respective IPv4 or IPv6 address of the virtual server.

Enabling DNS cache proxy

The **dns cache-proxy** command enables you to configure the GSLB ServerIron ADX to act as a proxy for the authoritative DNS (itself a virtual server configured on the controller) so that the GSLB ServerIron ADX responds directly to the client queries.

To enable DNS cache proxy, enter the following commands:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns cache-proxy
```

Syntax: **[no] dns cache-proxy**

Enabling DNS override

DNS override enables you to configure the GSLB ServerIron ADX to "override" the DNS reply for a domain and specify the IP addresses for the domains configured on it. DNS override (when configured in conjunction with DNS cache-proxy) allows the GSLB ServerIron ADX to respond directly to DNS queries using the configured IP lists, without the need for a backend DNS server.

To enable DNS override, use the **dns override** command. You must enable DNS override to allow the ServerIron ADX to insert the proxy IP address in the DNS reply.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns override
```

Syntax: [no] dns override

NOTE
Although DNS override is a global parameter. The response to the client contains all the domain IPs configured for the domain. You can enable the active-only option in the policy, in which case the reply contains only the active addresses. Refer to "Configuring an active-only policy" on page 229.

To display the DNS override state, enter the **show gslb policy** command. The state is shown in the DNS override field. Refer to "Displaying the default GSLB policy" on page 175 for more information.

NOTE
Both DNS cache-proxy and DNS override must be enabled to configure GSLB for IPv6.

Configuring zones

You must specify the DNS zone name and the host information (applications) within each zone for which you want the GSLB ServerIron ADX to provide global server load balancing. There are no defaults for these parameters.

To configure a zone, enter commands such as the following:

```
ServerIronADX(config)# gslb dns zone-name brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# host-info ftp ftp
```

This example adds the zone brocade.com and two host names within that zone: www and ftp. The GSLB ServerIron ADX will provide global SLB for these two hosts within the zone.

Syntax: [no] gslb dns zone-name <*name*>

The <*name*> parameter specifies the DNS zone name. If you delete a DNS zone (by entering **no gslb dns zone-name** <*name*>), the zone and all the host names you associated with the zone are deleted.

Syntax: [no] host-info <*host-name*> <*host-application*> | <*TCP/UDP-port-num*>

The <*host-name*> parameter specifies the host name. You do not need to enter the entire (fully-qualified) host name. Enter only the host portion of the name. For example, if the fully qualified host name is *www.brocade.com*, do not enter the entire name. Enter only "www". The rest of the name is already specified by the **gslb dns zone-name** command. You can enter a name up to 32 characters long.

The <*host-application*> parameter specifies the host application for which you want the GSLB ServerIron ADX to provide global server load balancing. You can specify one of the following:

- **FTP**: the well-known name for port 21. (Ports 20 and 21 both are FTP ports but on the ServerIron ADX, the name "FTP" corresponds to port 21.)
- **TFTP**: the well-known name for port 69
- **HTTP**: the well-known name for port 80
- **IMAP4**: the well-known name for port 143
- **LDAP:** the well-known name for port 389
- **NNTP:** the well-known name for port 119
- **POP3:** the well-known name for port 110
- **SMTP**: the well-known name for port 25
- **TELNET**: the well-known name for port 23

The <*TCP/UDP-port-num*> parameter specifies a TCP/UDP port number instead of a well-known port. If the application is not one of those listed above, you still can configure the GSLB ServerIron ADX to perform the Layer 4 health check on the specified port. If the application number does not correspond to one of the well-known ports recognized by the ServerIron ADX, the GSLB ServerIron ADX performs Layer 4 TCP or UDP health checks for the ports but does not perform application-specific health checks.

NOTE
For other applications (applications not listed above), the ServerIron ADX does not perform a Layer 7 heath check but still performs a Layer 3 or Layer 4 TCP or UDP health check. You can customize the HTTP health check on an individual host basis by changing the URL string the ServerIron ADX requests in the health check and the list of HTTP status codes the ServerIron ADX accepts as valid responses to the health check.

Specifying DNS override IP lists

Once you enable DNS override, you must configure a set of IP addresses (an IP list) for each domain name (zone and host) configured on the GSLB ServerIron ADX (GSLB controller).

You can specify as many IP addresses as you need for a given domain. When you specify multiple IP addresses, the GSLB ServerIron ADX uses the applicable GSLB policy metrics to select the best address from the list of addresses you configure. For information about the metrics, refer to "Configuring GSLB policy metrics for IPv6" on page 204.

Although DNS override is a global parameter. DNS override IP lists are associated with a specific host in a specific domain. To configure the proxy server information on the GSLB ServerIron ADX, enter commands such as the following:

```
ServerIronADX(config)# gslb dns zone brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# host-info www ip-list 2001:db8::56
```

The **host-info ip-list** command configures a list of IP addresses corresponding to host names for which the GSLB controller acts as the authoritative DNS server (ADNS). In the example, a single proxy server IPv6 address is specified for the zone called "brocade.com".

Syntax: **[no] host-info** <*host-name*> **ip-list** <*ipv6-address*>

The <*host-name*> parameter specifies the host name.

The **ip-list** <*ipv6-address*> variable specifies the proxy IPv6 address(es). You can specify as many proxy IP addresses as you need. If you specify multiple addresses, separate each address with a space. Here is an example:

```
host-info www ip-list 2001:db8::56 2001:db8::ab 2001:db8::cd
```

Configuring sites

The GSLB protocol is disabled by default. You must enable the GSLB protocol on each site ServerIron ADX. After you enable the GSLB protocol, the GSLB ServerIron ADX finds the site ServerIron ADXs using their IP management addresses, which you specify when you configure the remote site information.

When you create a site, you give it a name and identify the ServerIron ADXs in it. (You can also specify the administrative preference for site ServerIron ADXs. Refer to "Administrative preference metric" on page 220.)

To configure the server sites shown in Figure 12 on page 195, enter commands such as the following:

```
ServerIronADX(config)# gslb site US
ServerIronADX(config-gslb-site-US)# si-name slb-1 209.157.22.206
ServerIronADX(config)# gslb site EU
ServerIronADX(config-gslb-site-EU)# si-name slb-1 92.108.22.114
```

These commands configure two GSLB sites: one in the United States (US), the other in Europe (EU). Each site contain one ServerIron ADX (a site ServerIron ADX) that load balances traffic across server farms.

Syntax: [no] gslb site <*name*>

The <*name*> parameter is a text string that uniquely identifies the site on the GSLB ServerIron ADX. You can enter a string up to 16 characters long. The string can contain blanks. To use blanks, enclose the string in quotation marks.

Syntax: [no] si-name [<*name*>] <*ip-addr*> [<*preference*>]

The **si-name** <*name*> parameter specifies a unique name for the ServerIron ADX at the site. You can enter a string up to 16 characters long. The string can contain blanks. To use blanks, enclose the string in quotation marks. You can enter up to four pairs of ServerIron ADX names and IP addresses on the same command line. The <*name*> parameter is optional.

The <*ip-addr*> parameter specifies whether the remote site runs on the switch code or router code. If the remote site runs the switch code, enter the IP address configured on the site ServerIron ADX. If it runs the router code, then enter the VE IP address on the site ServerIron ADX.

In both cases, you must not enter a virtual IP address (VIP) configured on the ServerIron ADX or a source IP address added for source NAT.

NOTE
Only IPv4 addresses are supported for site ServerIron ADXs. All communication between the GSLB ServerIron ADX and the site ServerIron ADX is on IPv4.

Site ServerIron ADX configuration

Enabling the GSLB protocol

The GSLB protocol is disabled by default on site ServerIron ADX switches. You must enable the GSLB protocol on each site ServerIron ADX switch and configure the IP addresses of the site ServerIron ADX switches on the GSLB ServerIron ADX to enable the GSLB ServerIron ADX to establish communication with the site ServerIron ADX switches.

To enable the GSLB protocol on the site ServerIron ADXs, enter the following command:

```
ServerIronADX(config)#gslb protocol
```

Syntax: [no] gslb protocol

The ServerIron ADX uses TCP port 182 for the GSLB protocol by default. You can change the port number if needed. Refer to "Changing the protocol port number" on page 29.

You also can secure access to a ServerIron ADX by configuring Access Control Lists (ACLs). For example, you can configure ACLs to control access to the device on TCP port 182. See the "Access Control Lists (ACLs)" chapter of the *ServerIron ADX Security Guide.*

Basic configuration example

The following procedure demonstrates the configuration of a GSLB ServerIron ADX for performing IPv6 GSLB. The configuration describes to the example shown in Figure 12 on page 195.

Configuration on GSLB ServerIron ADX (GSLB controller)

First, configure a virtual IP address to represent the authoritative DNS server (ADNS) for the domain. Although you do not need a real DNS server when you configure the GSLB ServerIron ADX as a DNS cache proxy with DNS override, you still need to configure a virtual IP address for the ADNS. Clients send queries to the virtual IP address.

1. To add a virtual IP address to which the clients can send their DNS queries, enter a command such as the following:

```
ServerIronADX(config)# server virtual-name-or-ip dns6-vip 2001:DB8::200
ServerIronADX(config-vs-dns-proxy)# port dns
ServerIronADX(config-vs-dns-proxy)# exit
```

The command adds IP address 2001:DB8::200 as a virtual server, the ADNS. When clients send their DNS queries to this address, the GSLB controller processes the queries.

NOTE
The DNS VIP can also be IPv4 address.

2. Enable DNS cache proxy mode with DNS override mode:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns cache-proxy
ServerIronADX(config-gslb-policy)# dns override
```

In a DNS cache proxy with DNS override configuration, GSLB ServerIron ADX (the GSLB controller) itself acts as the authoritative DNS server for the configured zones. The gslb policy command changes the CLI to the GSLB policy configuration level.

DNS override allows the ServerIron ADX to replace the IP address in the DNS reply with the IP addresses you configure for the DNS cache proxy. These addresses are defined in the IP list.

Before specifying the IP list, you must define the hosts and their associated health checks (if applicable). You also must specify the host names and applications that you want to provide global server load balancing for. For example, assume that brocade.com contains the following host names and applications: www.brocade.com (HTTP) and ftp.brocade.com (FTP).

3. Specify a zone and host names within that zone.

```
ServerIronADX(config)# gslb dns zone-name brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www http
ServerIronADX(config-gslb-dns-brocade.com)# host-info ftp ftp
```

When you configure the GSLB ServerIron ADX, you also specify the zones for which you want the ServerIron ADX to provide global server load balancing. These are the zones for which the GSLB controller server is the authority (ADNS).

In this example, the GSLB ServerIron ADX is an authority for www.brocade.com and ftp.brocade.com. The GSLB ServerIron ADX will provide global server load balancing for these two.

The application specifies the type of health check the GSLB ServerIron ADX applies to IP addresses for the host. A host name can be associated with more than one application. In this case, the GSLB ServerIron ADX considers a host name's IP address to be healthy only if the address passes all the health checks.

4. Specify the IP list.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# host-info www ip-list 2001:db8::56 2001:db8:ab
```

You can specify as many domain IP addresses as you need for a given domain. When you specify multiple domain addresses, the GSLB ServerIron ADX uses the applicable GSLB policy metrics to select the best address from the list of addresses you configure and places that address at the top of the DNS reply.

5. Specify sites and the site ServerIron ADX within the sites on the GSLB ServerIron ADX:

```
ServerIronADX(config)# gslb site US
ServerIronADX(config-gslb-site-US)# si-name slb-1 209.157.22.206
ServerIronADX(config)# gslb site EU
ServerIronADX(config-gslb-site-EU)# si-name slb-1 92.108.22.114
```

Configuration on site ServerIron ADXs

6. Enable the GSLB protocol on each of the Site ServerIron ADXs:

```
ServerIronADX(config)# gslb protocol
```

The GSLB protocol is disabled by default on Site ServerIron ADX switches for security.

After you enable the GSLB protocol on the site ServerIron ADX switches, the GSLB ServerIron ADX finds the site ServerIron ADXs using their configured IP addresses, which you specify when you configure the remote site information.

If you have enabled the GSLB protocol on the site ServerIron ADXs, the GSLB ServerIron ADX begins communicating with the site ServerIron ADXs using the GSLB protocol as soon as you add the site definitions to the GSLB ServerIron ADX.

Advanced GSLB configuration for IPv6

Advanced configuration tasks include the configuration of GSLB policies and site persistence for IPv6 addresses.

Advanced configuration tasks include:

- **GSLB policy metrics for IPv6**: GSLB ServerIron ADX supports a subset of policy metrics for load balancing of IPv6 addresses.
- **Sticky persistence for IPv6**: GSLB ServerIron ADX supports sticky site persistence for IPv6 addresses. Refer to "Sticky persistence for IPv6" on page 222.
- **Hash-based persistence for IPv6**: GSLB ServerIron ADX supports hash-based site persistence for IPv6 addresses. For more information, refer to "Hash-based persistence for IPv6" on page 225.
- **Weighted hash-based persistence for IPv6**: GSLB ServerIron ADX supports weighted hash-based site persistence for IPv6 addresses. For more information, refer to "Weighted hash-based persistence for IPv6" on page 226.
- **DNS response parameters**: GSLB ServerIron ADX enables you to modify DNS-related GSLB parameters to restrict the number of IP addresses in the DNS response. For more information, refer to "Configuring DNS response parameters" on page 229.

Table 17 shows the advanced configuration tasks described in this section.

TABLE 17 Advanced GSLB for IPv6 configuration tasks

Feature	See page...
GSLB policy metrics	
Configuring GSLB policy metrics	page 204
Configuring the server (host) health metric	page 208
Configuring the weighted IP metric	page 211
Configuring the weighted site metric	page 211
Configuring the session capacity threshold metric	page 213
Configuring the active bindings metric	page 214
Configuring the active geographic location metric	page 216
Configuring the available session capacity metric	page 218
Configuring the FlashBack speed metric	page 219
Configuring the administrative preference metric	page 220
Configuring the least response time selection metric	page 221
Configuring the round robin selection metric	page 221
GSLB site persistence	
Configuring sticky persistence for IPv6	page 222

TABLE 17 Advanced GSLB for IPv6 configuration tasks

Feature	See page...
Configuring hash-based persistence for IPv6	page 225
Configuring weighted hash-based persistence for IPv6	page 226
DNS response parameters	
Configuring an active-only policy (optional)	page 229
Configuring an best-only policy (optional)	page 230

Configuring GSLB policy metrics for IPv6

The GSLB ServerIron ADX supports global server load balancing of IPv6 addresses in cache proxy with DNS override mode. In this mode, The GSLB ServerIron ADX evaluates each IP address in the IP list based on the configured policy metrics and places the best IP address on the top of the IP list in the response.

Table 18 lists the GSLB policy metrics used to load balance IPv6 addresses. The metrics are listed in their default order. If the GSLB controller is unable select the best IP address based on a metric, the candidate IP addresses are passed on to the next step in the GSLB algorithm, where the process of selecting the best IP address continues.

TABLE 18 GSLB policy metrics for IPv6

Metric	Default	Configuration options
Server (host) health	**Enabled.** The GSLB ServerIron ADX performs Layer 4 health checks on the TCP or UDP port and Layer 7 health checks on the application, if the application is known to the ServerIron ADX. NOTE: If all the sites fail their health checks, resulting in all the sites being rejected by the GSLB ServerIron ADX, the ServerIron ADX sends the DNS reply unchanged to the client.	You can disable this metric. NOTE: When both the health check metric and the FlashBack metric are is disabled, the ServerIron ADX does not perform any Layer 4 or Layer 7 health checks. Refer to "Server (host) health metric" on page 208.
Weighted IP address	**Disabled.** When enabled, the ServerIron ADX distributes GSLB traffic among IP addresses in the IP list based on weights assigned to the IP addresses.	You can disable this metric. You can enable this metric and assign weights to individual IP addresses. The weight can be a value from 0 to 100. The default value is 0. Refer to "Weighted IP metric" on page 209.

TABLE 18 GSLB policy metrics (Continued)for IPv6

Metric	Default	Configuration options
Weighted site metric	**Disabled.** When the weighted IP metric is enabled, the weighted site metric is disabled. The weighted site metric is an alternative to the weighted IP metric. They are mutually exclusive. When enabled, the ServerIron ADX distributes SLB traffic among GSLB sites based on weights configured for the sites.	You can disable this metric. You can enable this metric and assign weights to individual sites. The weight can be from 0 to 100. The default is 0. Refer to "Weighted site metric" on page 211.
Session capacity threshold	**Enabled.** The default value for the threshold is 90%. Thus, a site ServerIron ADX is eligible to be the best site only if its session utilization is below 90%.	You can disable this metric. You can change the threshold to a value from 0-100%. Refer to "To view the results of traffic distribution after configuring weighted site metrics, use the show gslob traffic site command. Refer to "Displaying results of traffic distribution for weighted sites" on page 235." on page 213.
Connection load	**Not supported.**	The connection load policy metric is not supported in the current implementation of GSLB for IPv6.
Active bindings	**Disabled.** When enabled, the ServerIron ADX selects an IP address with the highest number of active bindings as the best IP address for the client.	You can enable and disable this metric. Refer to "Active bindings metric" on page 214.
Round-trip time	**Not supported.**	The active and passive round-trip time policy metrics are not supported in the current implementation of GSLB for IPv6.
Geographic location	**Enabled.** The GSLB controller selects an IP address based on the geographic location of the server.	You can disable this metric. Refer to "Geographic location metric" on page 216.
Available session capacity	**Enabled.** The default tolerance is 10%. When comparing sites based on the session table utilization, the GSLB ServerIron ADX will prefer one site over the other only if the difference in session table utilization is greater than the tolerance percentage.	You can disable this metric. You can change the tolerance to a value from 0-100%. Refer to "Available session capacity metric" on page 218.

TABLE 18 GSLB policy metrics (Continued)for IPv6

Metric	Default	Configuration options
FlashBack speed	**Disabled.** The default tolerance is 10%. This applies to the TCP health check and application health checks. When comparing sites based on the FlashBack speed, the GSLB ServerIron ADX will prefer one site over the other only if the FlashBack speeds differ by more than the specified tolerance.	You also can disable this metric. You can change the TCP and application tolerances individually. A change applies to all the TCP ports or applications at the remote site. Refer to "FlashBack speed metric" on page 219.
Administrative preference	**Disabled.** When enabled, the default preference is 128. The GSLB ServerIron ADX will prefer the site with the highest administrative preference. If you set the preference for a site ServerIron ADX to 0, the site is administratively removed from GSLB selection.	You can enable this metric. On an individual site ServerIron ADX basis, you can change the preference from 128 (the default) to a value from 0-255. Refer to "Administrative preference metric" on page 220.
Least response selection	**Enabled.** The GSLB controller selects the site ServerIron ADX that has been selected less often than others.	Not configurable. Refer to "Least response selection metric" on page 221.
Round robin selection	**Disabled.** When round robin selection is enabled, the least response selection metric is disabled. round robin selection is an alternative to least response selection. They are mutually exclusive. Like least response selection, round robin selection is a tie breaker, used only if two or more sites are equal following comparison against all other enabled metrics.	Not configurable. Refer to "Round robin selection metric" on page 221.

All of these metrics have default values but you can change the values if needed. In addition, you can disable individual metrics or reorder them. Refer to "Changing the GSLB policy metrics" on page 34.

GSLB ServerIron ADX does not currently support the following GSLB policy metrics for IPv6 addresses:

- Active and passive round-trip time
- Connection load

Changing the order of GSLB for IPv6 policy metrics

You can change the order in which the GSLB ServerIron ADX applies the policy metrics.

NOTE
Brocade recommends that you always use the health check as the first metric. Otherwise, it is possible that the GSLB policy will not select a "best" choice, and thus send the DNS reply unchanged. For example, if the first metric is geographic location, and the DNS reply contains two sites, one in North America and the other in South America, for clients in South America the GSLB policy favors the South American site after the first comparison. However, if that site is down, the GSLB policy will find that none of the sites in the reply is the "best" one, and thus send the reply unchanged.

You cannot change the position of the least response selection or round robin selection metric, whichever is enabled. The GSLB ServerIron ADX uses the least response selection or round robin selection metric as a tie-breaker if the other comparisons do not result in selection of a "best" site.

To change the order, specify the metrics in the desired order by entering a command such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# metric-order set health-check capacity
num-session flashback
```

This command changes the GSLB policy to the following:

- The health check results
- The session capacity threshold (capacity) of the site ServerIron ADX
- The available session capacity threshold (num-session) of the site ServerIron ADX
- The FlashBack speed of the site ServerIron ADX
- The least response selection (the site ServerIron ADX that has been selected less often than others)

Two of the metrics, server health and geographic location, are not specified. As a result, these metrics are not used when evaluating site IP addresses in the DNS responses.

Syntax: [no] metric-order set <*list*>

The <*list*> parameter is a list of the metrics you want to use, in the order you want the GSLB ServerIron ADX to use them. The GSLB uses the metrics in the order you specify them. You can specify one or more of the following:

- **active bindings:** The ServerIron ADX's preference for the IP address with the highest number of active bindings.
- **capacity**: The session capacity threshold of the site ServerIron ADX.
- **flashback:** The FlashBack speed (how quickly the GSLB receives the health check results) of the site ServerIron ADX.
- **geographic:** The geographic location of the server.
- **health-check**: The Layer 4 and application health checks.
- **num-session**: The available session capacity of the site ServerIron ADX.
- **preference**: The administratively configured preference for the site ServerIron ADX.
- **weighted ip**: The administratively configured traffic distribution method for the ServerIron ADX.
- **weighted site:** The administratively configured traffic distribution method for the ServerIron ADX.

There are no parameters for the least response selection or round robin selection metrics. These metrics are tie-breakers. Only one of them is enabled at a time and the one that is enabled is always the last metric in the policy.

Resetting GSLB policy metrics

To reset the order of the GSLB policy metrics to the default (and also re-enable all disabled metrics), enter the following command.

```
ServerIronADX(config-gslb-policy)# metric-order default
```

Syntax: **metric-order default**

The **no metric-order set** command also resets the order and re-enables all disabled metrics. This command is equivalent to the **metric-order default** command.

To display the GSLB policy after you change it, enter the **show gslb policy** command. Refer to "Displaying the user-configured GSLB policy" on page 234.

Disabling or re-enabling individual GSLB policy metrics

You can explicitly disable individual GSLB policy metrics. For example, to disable the health check and geographic metrics, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# no health-check
ServerIronADX(config-gslb-policy)# no geographic
```

Syntax: **[no] health-check | num-session | preference | round-robin | geographic | capacity | flashback**

NOTE
If you explicitly disable both the health check and FlashBack metrics, the GSLB ServerIron ADX does not perform any health checks on the remote sites.

To enable a metric, enter the command without "no" in front of it. For example, to re-enable both the metrics disabled in the preceding example, enter the following commands:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# health-check
ServerIronADX(config-gslb-policy)# geographic
```

To enable the administrative preference metric, which is disabled by default, enter the following commands:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# preference
```

Server (host) health metric

The GSLB ServerIron ADX sends a Layer 3, Layer 4 TCP or UDP health check and Layer 7 application health check to the server to determine the health of the server and the host application on the server. If the server fails either health check, the GSLB ServerIron ADX immediately disqualifies the server's IP address from being the "best" site.

When you configure a ServerIron ADX for GSLB, it learns a series of IP addresses from its configured DNS real servers. Then it performs Layer 3, Layer 4, and if possible, Layer 7 health checks against those IP addresses.

The GSLB ServerIron ADX determines which health checks to use based on the host applications you specify. For example, if a host name is associated with both HTTP and FTP applications, the ServerIron ADX sends the site Layer 4 TCP health checks (one for HTTP and one for FTP) and also sends a separate Layer 7 HTTP health check and a separate Layer 7 FTP health check. The site must pass all the health checks or it is disqualified from being the best site.

If a host application uses a port number that is not known to the ServerIron ADX and supported by GSLB, the ServerIron ADX cannot perform a Layer 7 health check on the application but still performs a Layer 4 TCP or UDP health check on the port. Health check parameters such as retry interval, number of retries, and so on are global parameters.

Weighted IP metric

GSLB ServerIron ADX supports the weighted IP policy metric for load balancing of IPv6 addresses. When enabled, the GSLB controller distributes GSLB traffic among IP addresses in the IP list, based on weights assigned to the IP addresses.

The weight configured for an IP address determines the percentage of traffic that a IP address receives in comparison with other candidate IP addresses, which may or may not have assigned weights.

Using the weighted IP metric, the GSLB algorithm calculates a relative weight for each IP address and selects the IP address with the *least relative weight*.

The following criteria are used to calculate the relative weight of each IP address:

- The number of times the GSLB ServerIron ADX selected the IP address as the best IP address to reply to a client
- The number of eligible IP addresses to be evaluated by the weighted IP metric and their weights
- The weight assigned to the IP address

If an IP address has a relative weight of zero, or if it does not have a weight assigned to it, the IP address is not selected as the best IP address for a client.

If two or more IP addresses have the same relative weight, or if all of the IP addresses have a relative weight of zero, all of the IP addresses with the same relative weight are passed on to the next step in the GSLB algorithm, where the process of selecting the best IP address continues.

NOTE
The weighted IP metric is disabled by default. Once enabled, it is placed second in the GSLB algorithm, after the health check metric. You can change the metric order and enable or disable other metrics, although Brocade does not recommended this. "Changing the order of GSLB for IPv6 policy metrics" on page 206.

Enabling the weighted IP metric

To configure weighted IP metrics, you must enable the weighted IP metric and specify the weights of IP addresses.

For example, you could add the zone gslb.com, add the host www within the gslb.com zone, and assign a weight of 50 to the IP address 2001:DB8::56 by entering commands such as the following:

```
SLB-ServerIronADX(config-gslb-policy)# weighted-ip
SLB-ServerIronADX(config-gslb-policy)# gslb dns zone gslb.com
SLB-ServerIronADX(config-gslb-dns-gslb.com)# host www http
SLB-ServerIronADX(config-gslb-dns-gslb.com)# host www ip-weight 2001:db8::56 50
```

Syntax: **[no] weighted-ip**

Syntax: **[no] gslb dns zone** <*name*>

For <*zone-name*>, enter up to 32 characters.

Syntax: **[no] host-info** <*host-name*> <*host-application*> | <*tcp/udp-portnum*>

The <*host-name*> variable specifies the host name. You do not need to enter the entire fully qualified host name. Enter only the host portion of the name. For example, if the fully qualified host name is *www.gslb.com*, do no enter the entire name. Enter only "www". The rest of the name is already specified by the **gslb dns zone** command.

The <*host-application*> parameter specifies the host application for which you want to create an IP list. Specify one of the following:

- **ftp**: the well-known name for port 21. (Ports 20 and 21 both are FTP ports but on the ServerIron ADX, the name “ftp” corresponds to port 21.)
- **tftp**: the well-known name for port 69
- **http:** the well-known name for port 80
- **imap4:** the well-known name for port 143
- **ldap**: the well-known name for port 389
- **nntp**: the well-known name for port 119
- **pop3**: the well-known name for port 110
- **smtp:** the well-known name for port 25
- **telnet:** the well-known name for port 23

Specifying the weight of IP addresses in the IP list

To specify the weight given to an IPv6 address, use the **host-info ip-weight** command and its operands to identify the host, the IPv6 address, and the weight.

Enter a command such as the following:

```
ServerIronADX(config)# gslb dns zone brocade.com
ServerIronADX(config-gslb-dns-brocade.com)# host-info www ip-weight 2001:db8::56
10
```

The command in the example specifies a weight of 10 for the IPv6 address.

Syntax: **[no] host-info** <*host-name*> **ip-weight** {<*ipv6-address*> <*weight*>}

The <*host-name*> variable specifies the host name under the zone. Again, you do not need to enter the entire fully qualified host name. Enter only the host portion of the name.

The <*ipv6-address*> variable specifies the proxy IPv6 address(es) to which you are assigning a weight. The <*weight*> is a value from 0 to 100. The default value is 0.

The command results in an “IP-address not found for host-name” error if the IPv6 address specified for the **ip-weight** parameter was not used as an argument when you defined the IP list. For information about specifying IP lists, see “Specifying DNS override IP lists” on page 199.

NOTE
If no IP list is defined for the host, the IP weight for the host IPs are removed from the GSLB DNS zone configuration whenever the GSLB ServerIron ADX reloads.

Use the **show gslb dns** command to view information about the distribution of traffic after the configuration of weighted IP metrics. For more informaiton see “Displaying DNS zone and hosts” on page 237.

Weighted site metric

You can configure the ServerIron ADX to distribute SLB traffic among GSLB sites based on weights configured for the sites. The weights determine the percentage of traffic each site will receive in comparison with other sites, which may or may not have weights.

NOTE
You cannot use the weighted site metric if the weighted IP metric is enabled. You assign weights to GSLB sites. Each GSLB site may consist of one or more ServerIron ADXs, but the weight is applicable to the site as a whole.

The GSLB ServerIron ADX uses relative percentages in order to achieve 100% total weight distribution.

You can configure the ServerIron ADX to distribute SLB traffic among GSLB sites based on weights configured for the sites. The weights determine the percentage of traffic each site will receive in comparison with other sites, which may or may not have weights.

The GSLB ServerIron ADX uses relative percentages in order to achieve 100% total weight distribution, as shown in Table 19 and Table 20. In Table 19, the total of the Configured weighted site metrics (second column) is 100. The last column shows that the GSLB ServerIron ADX distributes the traffic to the IP addresses exactly as configured. In this example, traffic distribution is straightforward because the total weight of all three GSLB sites equals 100.

TABLE 19 Example weighted site metric configuration

GSLB site	Configured weighted site metric	Relative weighted site metric
San Jose	50	50%
New York	30	30%
London	20	20%
Total	100	100%

Now consider the example in Table 20. In this example, the total of the configured weighted site metrics (second column) does not equal 100. However, as illustrated in the last column, the GSLB ServerIron ADX uses relative percentages in order to achieve 100% total weight distribution.

TABLE 20 Example weighted site metric configuration

IP address	Configured weighted site metric	Relative weighted site metric
San Jose	15	33% (15/45 * 100)
New York	20	44% (20/45 * 100)
London	10	22% (10/45 * 100)
Total	45	100%

By default, the weighted site metric is disabled. When enabled, it is placed second in the GSLB algorithm, after the server (host) health metric. You can change the metric order and enable or disable other metrics, although we do not recommend this. For more information, refer to "Changing the order of GSLB for IPv6 policy metrics" on page 206.

DNS response processing

When the weighted site metric is enabled, the GSLB ServerIron ADX selects an IP address belonging to a particular site to be the best IP address in the DNS reply to a client. The client subsequently makes an SLB request to that IP address.

Using the weighted site metric, the GSLB algorithm calculates a relative weight for each IP address and selects the IP address with the least relative weight. The GSLB ServerIron ADX uses the following criteria to calculate the relative weight of an IP address:

- The number of times the GSLB ServerIron ADX selected the IP address as the best IP address to reply to a client
- The number of eligible IP addresses to be evaluated by the weighted site metric, and the weights of sites to which they belong
- A calculated weight assigned to an IP address, based on the following criteria:
  - If the IP address is a real server, then the calculated weight is zero
  - If the IP address is a virtual IP (VIP), the weight is calculated based on the site the VIP belongs to, the weight of the site, and the number of candidate VIPs belonging to the site and being evaluated by the weighted site metric

If an IP address has a relative weight of zero, or if an IP address belongs to a site that does not have an assigned weight, the IP address is not selected as the best IP address for a client. Note that all real servers have a relative weight of zero, as do VIPs that belong to sites with no assigned weights.

If two or more IP addresses have the same relative weight, or if all of the IP addresses have a relative weight of zero, all of the IP addresses with the same relative weight are passed on to the next step in the GSLB algorithm, where the process of selecting the best IP address continues.

Traffic distribution specifications

In general, DNS response selection counters are maintained per IP address, per domain name. For example, suppose you configure three GSLB sites with assigned weights. All three sites host the application *www.gslb.com* and sites New York and London also host ftp.gslb.com, as illustrated below.

www.gslb.com
VIP 2001:DB8::1 belongs to San Jose with a weight of 50
VIP 2001:DB8::2 belongs to New York with a weight of 30
VIP 2001:DB8::3 belongs to London with a weight of 20

ftp.gslb.com
VIP 2001:DB8::2 belongs to New York with a weight of 30
VIP 2001:DB8::3 belongs to London with a weight of 20

Suppose that ten DNS requests are made to *www.gslb.com*. By viewing the selection counters (using the **show gslb dns zone** command), you would see that San Jose is selected five times (50%), New York is selected three times (30%), and London is selected two times (20%).

Now suppose that five DNS requests are made to ftp.gslb.com. In this case, New York receives three requests (60%), and London receives two requests (40%). This is because counters are maintained per IP address per domain name.

If you consider the total site traffic for both applications, the traffic distribution is as follows: San Jose = 5 (33%); New York = 6 (40%); and London = 4 (26%). The GSLB ServerIron ADX evaluates the results of the weighted metrics with respect to a specific domain name, not an IP address alone.

Configuring weighted site metrics

To configure weighted site metrics, complete the following tasks:

1. Enable the weighted site metric.
2. Select the site for which to apply weights.
3. Configure a weight for the site.

For example, enter commands such as the following:

```
ServerIronADX(config-gslb-policy)# weighted-site
ServerIronADX(config-gslb-policy)# gslb site SanJose
ServerIronADX(config-gslb-site-SanJose)# weight 50
```

Syntax: [no] weighted-site

Syntax: **gslb site** <*site name*>

The <*site name*> can have a maximum of 16 characters.

Syntax: **weight** <*weight*>

The <*weight*> is a value from 0 to 100. The default value is 0.

To view the results of traffic distribution after configuring weighted site metrics, use the **show gslob traffic site** command. Refer to “Displaying results of traffic distribution for weighted sites” on page 235.

Session capacity threshold metric

The GSLB protocol supplies statistics for the session tables on each site ServerIron ADX. The session table contains an entry for each open TCP or UDP session on the site ServerIron ADX. Each ServerIron ADX has a maximum number of sessions that it can hold in its session table. Through the GSLB protocol, the GSLB ServerIron ADX learns from each remote ServerIron ADX the maximum number of sessions and the number of available sessions on that ServerIron ADX.

The capacity threshold specifies how close to the maximum session capacity the site ServerIron ADX (remote ServerIron ADX) can be and still be eligible as the best site for the client. This mechanism provides a way to shift load away from a site before the site becomes congested.

The default value for the threshold is 90%. Thus a site ServerIron ADX is eligible to be the best site only if its session utilization is below 90%. Refer to "Displaying DNS zone and hosts" on page 237 for commands to display a site's utilization and the capacity threshold.

Active bindings metric

You can configure the ServerIron ADX to prefer an IP address with the highest number of active bindings.

Active bindings are a measure of the number of active real servers bound to a virtual IP address (VIP) residing on a GSLB site. The GSLB ServerIron ADX uses the active bindings metric to select the best IP address for the client. The VIP with the highest number of active bindings is the IP address preferred by the active bindings metric.

NOTE
By default, the active bindings metric is disabled. Once enabled, it is placed after the available session capacity metric in the GSLB algorithm. You can change the metric order or enable or disable other metrics, although we do not recommend this.

DNS response processing

When the active bindings metric is enabled, the GSLB ServerIron ADX evaluates each IP address in the DNS reply from the server, and selects the IP address with the highest number of active bindings. The client subsequently makes an SLB request to that IP address.

Active bindings are calculated as follows:

- If the IP address is a VIP residing on a remote site that supports active bindings, then the number of active bindings equals the number of active real servers bound for application ports.
- If the IP address is a VIP residing on a remote site that is running older versions of the GSLB agent software, and consequently does not support the active bindings metric, then the number of active bindings for the IP address is 1 or 0, depending on the health of the VIP.
- If the IP address is a real server, then the number of active bindings for the IP address is 1 or 0, depending on the health of the real server.

If all IPs or VIPs have zero active bindings, or if all IPs or VIPs have the same number of active bindings, the GSLB ServerIron ADX passes them on to the next step in the GSLB algorithm, where the process of selecting the best IP address continues. Likewise, if two or more IP addresses have the highest maximum value of active bindings, the GSLB ServerIron ADX passes them on to the next step in the GSLB algorithm.

Enabling active bindings

Active bindings are a measure of the number of active real servers bound to a virtual IP address (VIP) residing on a GSLB site. The GSLB ServerIron ADX uses the active bindings metric to select the best IP address for the client. The VIP with the highest number of active bindings is the IP address preferred by the active bindings metric.

To configure the active bindings metric, enter the following command:

```
ServerIronADX(config-gslb-policy)# active-bindings
```

Syntax: [no] active-bindings

Use the **show gslb dns detail** command to view the active bindings for each IP address. Refer to "Displaying DNS zone and hosts" on page 237 for sample output.

Configuring weighted active bindings

Weighted active bindings allows you to configure the GSLB ServerIron ADX to direct requests to domain VIPs in proportion to their active bindings.

For example, if VIP-1 has two active bindings and VIP-2 has one active binding, you can configure the GSLB ServerIron ADX to direct two-thirds of the client requests to VIP-1 and one-third of the client requests to VIP-2.

To enable weighted active bindings for the global GSLB policy, first enable the active bindings using the existing **active-bindings** CLI command, then configure the following additional command:

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# weighted-selection
ServerIronADX(config-gslb-policy)# end
ServerIronADX#
```

To enable weighted active bindings for the host level policy, first enable the active bindings using the existing **active-bindings** CLI command, then configure the following additional command:

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb-host-policy abc
ServerIronADX(config-gslb-host-policy-abc)# weighted-selection
ServerIronADX(config-gslb-host-policy-abc)# end
ServerIronADX#
```

Using minimum active bindings

You can configure the GSLB ServerIron ADX to use the minimum active bindings among all application ports if multiple application ports are associated with a domain. For example, if application ports http and ftp are configured for *www.companynet.com*, you may need the active bindings count for the VIPs to be based on the minimum of the active bindings for these two application ports. You can configure the GSLB ServerIron ADX to use minimum bindings as follows:

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb dns zone companynet.com
ServerIronADX(config-gslb-dns-companynet.com)# host-info www http
ServerIronADX(config-gslb-dns-companynet.com)# host-info www ssl
ServerIronADX(config-gslb-dns-companynet.com)# host-info www min-bindings
ServerIronADX(config-gslb-dns-companynet.com)# end
```

Tracking an application port for active bindings

You can configure the GSLB ServerIron ADX to track a particular application port for active bindings if multiple application ports are associated with a domain. For example, if application ports HTTP and SSL are configured for *www.companynet.com*, you may need the active bindings count for the VIPs to be based only on the active bindings for the HTTP port but not the SSL port. You can configure the GSLB ServerIron ADX to track active bindings for the http port only as follows:

```
ServerIronADX# configure terminal
ServerIronADX(config)# gslb dns zone company.com
ServerIronADX(config-gslb-dns-company.com)# host-info www http
ServerIronADX(config-gslb-dns-company.com)# host-info www ssl
ServerIronADX(config-gslb-dns-company.com)# host-info www http track-port
ServerIronADX(config-gslb-dns-company.com)# end
```

Geographic location metric

ServerIron ADX GSLB policies use a number of metrics, including the geographic location of a server, to evaluate the server IP addresses in an IP list.

Once you configure a geographic region for an IP address prefix, the GSLB ServerIron ADX determines the geographic region of a server in the following ways:

- For a real address, the geographic region is based on the IP address. If you configure a geographic prefix that matches the real server IP address, the device obtains the geographic location of the real server from the geographic prefix entry that you configure.
- For a virtual IP address (VIP), the geographic region is based on the management IP address of the site ServerIron ADX on which the VIP is configured. If you configure a geographic prefix that matches the management IP address of the site ServerIron ADX on which the VIP is configured, the device obtains the geographic location of the VIP from the geographic prefix entry that you configure.
- If the management IP address of the remote ServerIron ADX at that site is not indicative of the geographic location, use the **geo-location** command to specify the region of the GSLB site. For more information about this command, see the “Specifying site locations” on page 217. For example, if the management IP address is in a private subnet, the address is not indicative of the ServerIron ADX’s geographic location. If you specify the region for the GSLB site, the GSLB ServerIron ADX uses the region you specify instead of the region of the ServerIron ADX’s management IP address.
- If you configure a geographic prefix entry that matches the management IP address of the remote ServerIron ADX and also specify a geographic location for the GSLB site where the remote ServerIron ADX resides, then the geographic location configured for the GSLB site takes precedence over the one defined in the user-configured geographic prefix entry. For example, the geographic region for a VIP configured on the remote ServerIron ADX will be obtained from the geographic location configured for the GSLB site where the remote ServerIron ADX resides instead of the geographic prefix entry that matches the management IP address of the remote ServerIron ADX.

The GSLB ServerIron ADX determines the geographic location of the client as follows: For each client query, the GSLB ServerIron ADX determines the geographic location from which the client query came based on its IP address.

- If the IP address prefix of a user-configured geographic prefix entry matches that of the client, then the geographic location of the client will be as specified in the user-configured geographic prefix entry.
- If multiple server IP addresses compare equally based on the GSLB metrics above the geographic metric in the GSLB policy, then the GSLB ServerIron ADX prefers server IP addresses within the same geographic region as the client query.

Configuring a geographic prefix

Using the **geo-prefix** command, you can configure the geographic location of an IP address prefix, or override an existing geographic region for an IP address prefix by configuring a new one.

You can assign one of the following geographic locations to an IP address prefix:

- North America
- South America
- Europe
- Asia
- Africa

To configure a geographic prefix, enter commands such as the following:

```
GSLB-ServerIronADX# configure terminal
GSLB-ServerIronADX(config)# gslb policy
GSLB-ServerIronADX(config-gslb-policy)# geo-prefix 2001.db8::/64 asia
GSLB-ServerIronADX(config-gslb-policy)# end
```

These commands create a geographic prefix entry with IPv6 address 2001.db8::, prefix length 64, and geographic region Asia.

Syntax: **[no] geo-prefix** *<ipv6-prefix>* **[asia | europe | n-america | s-america | africa]**

The command configures an association between a prefix and a geographic location. The *<ipv6-prefix>* variable identifies the respective networks. Five operands serve as location tags for the network: **asia**, **europe**, **n-americ**a, **s-america**, and **africa**.

NOTE
When a geographic prefix is converted from static to dynamic through geographic prefix configuration, the old geographic prefix information will be replaced with the new information. If the prefix is deleted, the old value will not be restored because it has already been replaced.

Specifying site locations

By default, the GSLB ServerIron ADX uses a site's IP address to determine its geographic location. Alternatively, you can explicitly specify the location, by entering commands such as the following:

```
ServerIronADX(config)# gslb site us
ServerIronADX(config-gslb-site-us)# geo-location n-america
```

Syntax: **[no] geo-location asia | europe | n-america | s-america | africa**

Specifying GSLB controller locations

By default, the GSLB controller is assigned to the North America geographic. Specify the GSLB controller location by entering commands such as the following at the global configuration level:

```
ServerIronADX(config)# gslb default-location asia
ServerIronADX(config)# write memory
```

The command specifies "asia" as the default location of the GSLB controller.

Syntax: **[no] gslb default-location asia | europe | n-america | s-america | africa**

If GSLB default location is not specified and if the requesting client prefix is from an unknown geography, then the GSLB controller assigns "north-america" as its geography. However, if the default location is specified, the GSLB controller assigns the configured geography to unknown client prefixes.

NOTE
This command requires a reload to take effect; therefore, always issue the **write memory** command after configuring the command.

Enabling default geographic location

The **use-default-location** command enables you to ensure that the geographic policy metric is used to load balance client requests even if the client prefix cache maintained by the GSLB ServerIron ADX is full.

By default, the GSLB ServerIron ADX ignores the default location of new client requests if its client prefix cache if full. Whenever the GSLB ServerIron ADX cannot create a new entry in the client prefix cache because it has already exceeded the limit, it ignores the geographic policy metric and falls to the next metric in the GSLB policy.

If the **use-default-location** command is configured for either the global GSLB policy or the host-level GSLB policy, the ServerIron ADX uses the default location of the client and the geographic policy metric when determining how to distribute the client's request.

To ensure that the geographic policy metric is used, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# use-default-location
```

The default location of the client corresponds to the default location configured on the GSLB controller. If no default location is configured on the GSLB controller, then n-america is assigned by default. For more information, see "Specifying GSLB controller locations" on page 217.

To view geographic policy metric settings see "Displaying information about a geographic prefix" on page 235 and "Displaying DNS zone and hosts" on page 237.

Available session capacity metric

If multiple sites are equal after the above comparisons, the GSLB ServerIron ADX prefers the site ServerIron ADX (remote ServerIron ADX) whose session table has the most unused entries.

When comparing sites based on the session table utilization, the GSLB ServerIron ADX considers the sites to be equal if the difference in session table utilization does not exceed the tolerance percentage. The tolerance percentage ensures that minor differences in utilization do not cause frequent, and unnecessary, changes in site preference.

For example, suppose one ServerIron ADX has 1 million sessions available, and another has 800,000 sessions available. Also assume that the tolerance is 10% (the default). In this case the first ServerIron ADX (with 1 million sessions available) is preferred over the second ServerIron ADX because the difference (200,000) is greater than 10% of 1 million. If a third ServerIron ADX has 950,000 sessions available, that ServerIron ADX is equally preferable with the first ServerIron ADX (with 1 million sessions available), because the difference in percentage between the available sessions on the two ServerIron ADXs is only 5%, which is less than the tolerance threshold.

You can change the following parameters associated with the session-table metrics:

- **Session capacity threshold**: Specifies how close to the maximum session capacity the site ServerIron ADX (remote ServerIron ADX) can be and still be eligible as the best site for the client. This mechanism provides a way to shift load away from a site before the site becomes congested. The default value for the threshold is 90%. Thus a site ServerIron ADX is eligible to be the best site only if its session utilization is below 90%.
- **Available session capacity tolerance**: Specifies the percentage by which the number of available sessions on the site ServerIron ADX can differ from the number of available sessions on another site ServerIron ADX and still be considered an equally good site.

You can change these parameters on an individual basis.

To change the session-table capacity metric, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# capacity threshold 99
```

Syntax: [no] capacity threshold <*num*>

The <*num*> parameter specifies the maximum percentage of a site ServerIron ADX's session table that can be in use. If the ServerIron ADX's session table utilization if greater than the specified percentage, the GSLB ServerIron ADX prefers other sites over this site. You can specify a percentage from 0-100. The default is 90.

To change the session-table tolerance metric, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# num-session tolerance 20
```

Syntax: [no] num-session tolerance <*num*>

The <*num*> parameter specifies the maximum percentage by which the session table utilization on ServerIron ADXs at different sites can differ without the GSLB ServerIron ADX selecting one over the other based on this metric. You can specify a tolerance from 0-100. The default is 10.

FlashBack speed metric

If multiple sites compare equally based on all the metrics above, the ServerIron ADX chooses a site as the best one based on how quickly the GSLB ServerIron ADX received responses to health checks to the site ServerIron ADX.

The GSLB ServerIron ADX uses a tolerance value when comparing the FlashBack speeds of different sites. The tolerance value specifies the percentage by which the FlashBack speeds of the two sites must differ in order for the ServerIron ADX to choose one over the other. The default FlashBack tolerance is 10%. Thus, if the FlashBack speeds of two sites are within 10% of one another, the ServerIron ADX considers the sites to be equal. However, if the speeds differ by more than 10%, the ServerIron ADX prefers the site with the lower FlashBack speed.

FlashBack speeds are measured at Layer 4 for all TCP/UDP ports. For the application ports known to the ServerIron ADX, the FlashBack speed of the application is also measured.

When the ServerIron ADX compares the FlashBack speeds, it compares the Layer 7 (application-level) FlashBack speeds first, if applicable. If the application has a Layer 7 health check and if the FlashBack speeds are not equal, the ServerIron ADX is through comparing the FlashBack speeds. If a host is associated with multiple applications, the GSLB ServerIron ADX uses the slowest response time among the applications for the comparison. However, if only the Layer 4 health check applies to the application, or if further tie-breaking is needed, the ServerIron ADX then compares the Layer 4 FlashBack speeds.

You can modify the following FlashBack parameters:

- Application tolerance
- TCP tolerance

The GSLB ServerIron ADX uses a tolerance value when comparing the FlashBack speeds of different sites. The tolerance value specifies the percentage by which the FlashBack speeds of the two sites must differ in order for the ServerIron ADX to choose one over the other. The default FlashBack tolerance is 10%. Thus, if the FlashBack speeds of two sites are within 10% of one another, the ServerIron ADX considers the sites to be equal. However, if the speeds differ by more than 10%, the ServerIron ADX prefers the site with the lower FlashBack speed.

FlashBack speeds are measured at Layer 4 for all TCP/UDP ports. For the application ports known to the ServerIron ADX, the FlashBack speed of the application is also measured.

When the ServerIron ADX compares the FlashBack speeds, it compares the Layer 7 (application-level) FlashBack speeds first, if applicable. If the application has a Layer 7 health check and if the FlashBack speeds are not equal, the ServerIron ADX is through comparing the FlashBack speeds. However, if only the Layer 4 health check applies to the application, or if further tie-breaking is needed, the ServerIron ADX then compares the Layer 4 FlashBack speeds.

To change the tolerances for the response times of TCP and application health checks, when used as a metric for selecting a site, enter commands such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# flashback application tolerance 30
ServerIronADX(config-gslb-policy)# flashback tcp tolerance 50
```

Syntax: [no] flashback application | tcp tolerance <*num*>

The **application | tcp** parameter specifies whether you are modifying the tolerance for the Layer 4 TCP health check or the Layer 7 application health checks. You can change one or both and the values do not need to be the same. For each, you can specify from 0-100. The default for each is 10.

Administrative preference metric

The administrative preference is an optional metric. This metric is a numeric preference value from 0-255 that you assign to each site ServerIron ADX, to select that ServerIron ADX if the previous metrics do not result in selection of a best site. The GSLB policy prefers the site ServerIron ADX with the highest administrative preference value.

The administrative preference allows you to do the following:

- You can temporarily change the preference of a site to accommodate changing network conditions. For example, if sites are offering proxy content service, the link between a site proxy server farm and the content origin may be highly congested, making that site less desirable. This factor is not visible to the ServerIron ADXs and thus cannot be reflected in the other GSLB metrics.
- You can temporarily disqualify a site ServerIron ADX from being selected, without otherwise changing the site's configuration or the GSLB ServerIron ADX's configuration. For example, you can perform maintenance on the site ServerIron ADX without making network changes. In this case, set the administrative preference to 0.

- You can bias a GSLB ServerIron ADX that is also configured as a site ServerIron ADX (for locally configured VIPs) to always favor itself as the best site. In this case, assign an administrative preference of 255 to the site for the GSLB ServerIron ADX itself, and assign a lower administrative distance to the other site ServerIron ADXs, or use the default (128) for those sites.

NOTE
The administrative preference metric is disabled by default and must be enabled before it is used in the GSLB policy algorithm. Once enabled, it is placed after the available session capacity metric. Refer to "Disabling or re-enabling individual GSLB policy metrics" on page 208.

Configuring administrative preference for a site

Once enabled, the default administrative preference for sites is 128. You can change the preference on an individual site basis.

Typically, you can set the administrative preference for a site ServerIron ADX when you define a site. For example, to set the administrative preference for a site ServerIron ADX to 255, enter a command such as the following:

```
ServerIronADX(config)# gslb site us
ServerIronADX(config-gslb-site-us)# si-name slb-1 2001:db8::56 255
```

To change the preference for a site ServerIron ADX you have already configured, use the same command syntax. You do not need to reconfigure other site parameters when you change the preference. For example, to change the preference for a site ServerIron ADX from the default (128) to 200, enter a command such as the following:

```
ServerIronADX(config)# gslb site us
ServerIronADX(config-gslb-site-us)# si-name slb-2 2001:db8::56 255 200
```

Least response selection metric

If multiple sites still compare equally based on all the metrics above, the GSLB ServerIron ADX selects the site that it has selected least often before. For example, if the GSLB ServerIron ADX has selected Site 1 and placed its IP address on top in 40% of the DNS replies, but has selected Site 2 60% of the time, then in this instance the GSLB ServerIron ADX selects Site 1. To display the response selection percentages for the sites you have configured, use the **show gslb dns zone** command. Refer to "Displaying DNS zone and hosts" on page 237.

This metric is a tie-breaker in case multiple addresses pass through all the above comparisons without one address emerging as the best choice. If this occurs, the address of the site that has been selected least often in previous DNS responses is selected.

Least response selection is enabled by default. You can disable the metric only by enabling the round robin selection metric to act as the tie breaker instead. See the following section.

Round robin selection metric

The round robin selection metric is an alternative to the least response selection metric as the final tie breaker. When you enable round robin selection, the GSLB ServerIron ADX automatically disables the least response selection metric, and instead uses the round robin algorithm to select a site. Round Robin selection chooses the first IP address in the DNS response for the first client request, then selects the next address for the next client request, and so on.

Use the round robin selection metric instead of the least response selection metric when you want to prevent the GSLB ServerIron ADX from favoring new or recently recovered sites over previously configured active sites. The least response selection metric can cause the GSLB ServerIron ADX to select a new site or a previously unavailable site that has come up again instead of previously configured sites for a given VIP. This occurs because the GSLB ServerIron ADX has selected the new site fewer times than previously configured sites for the VIP.

In some cases, the least response selection metric can cause the GSLB ServerIron ADX to send client requests to a new or recovered site faster than the site can handle while it is coming up. To avoid this situation, you can configure the GSLB ServerIron ADX to use the round robin selection metric instead of the least response selection metric as the final tie breaker.

The round robin selection metric is disabled by default.

Check the current and maximum values for GSLB resources using the **show gslb resource** command. If you are configuring more than 256 zones or configuring more than 600 hosts, perform the following tasks:

1. Change the maximum virtual server system parameter to the maximum value supported in the current release. Use the **l4-virtual-server** command.

   For the current maximum virtual server value supported, see the table named "The Number of Supported Real Servers, Virtual Servers and Ports" in the *ServerIron ADX Server Load Balancing Guide*.

2. Change the maximum real server system parameter to the maximum value supported in the current release. Use the **l4-real-server** command.

   For the current maximum real server value supported, see the table named "The Number of Supported Real Servers, Virtual Servers and Ports" in the *ServerIron ADX Server Load Balancing Guide*.

3. Change the maximum server port parameter to the maximum value supported in the current release. Use the **l4-server-port** command.

   For the current maximum server port value supported, see the table named "The Number of Supported Real Servers, Virtual Servers and Ports" in the *ServerIron ADX Server Load Balancing Guide*.

4. Check your system parameter values using the **show default value** CLI command.

NOTE
The sum of number of VIPs configured and the number of GSLB hosts configured on the GSLB ServerIron ADX should not exceed 1024. Similarly, the sum of real servers configured and the number of DNS IP addresses should not exceed 4096.

Sticky persistence for IPv6

GSLB ServerIron ADX offers two methods for site persistence: sticky persistence and hash-based persistence. Sticky persistence is the best solution for site persistence in single-box and High Availability (hot standby, symmetric active-standby, symmetric active-active) topologies.

NOTE
Hash-based persistence is a better choice for GSLB configurations that utilize two GSLB controllers (that are not in an HA configuration) for the same domain and where site persistence is needed for a single client that is directed to two GSLB controllers. For more information, see "Hash-based persistence for IPv6" on page 225

Sticky persistence enables the GSLB controller to ensure that the same IP address is sent to a client sending multiple DNS requests within a configurable period of time. Site persistence is particularly important in instances where user-specific content is stored at one site (such as a shopping cart) and redirection to another site would result in a lost session. Sticky persistence enables the GSLB controller to ensure that the client is directed to the site that was previously visited.

To return the same IP address for a client that has sent requests previously, the GSLB controller must save the following information:

- Client IP address/prefix
- Domain name the client requested
- Selected IP address for the request

This information is saved in a session table when the sticky GSLB persistence is enabled, and the GSLB controller creates a sticky session for each client within the session table. Each session has a special user type and source port or destination port number to distinguish from other sessions.

When a new request enters the system, the GSLB controller searches for the client IP and domain name pair. If a match is found, the previously selected IP address will be returned.

To ensure the selected IP is still valid for the request, the GSLB controller checks for the following conditions to be true before it returns the reply:

- Selected IP still belongs to the requested domain
- Selected IP is still active

Enabling sticky persistence for IPv6

Sticky persistence for IPv6 addresses is implemented as a GSLB policy, and it can be applied globally or on per-host basis.

To enable GSLB globally for all domains, enter commands such as the following on the GSLB controller:

```
SLB-Ctrl-ServerIronADX(config)#gslb policy
SLB-Ctrl-ServerIronADX(config-gslb-policy)#sticky
```

To enable Sticky GSLB for a specific host, enter commands such as the following on the GSLB controller:

```
SLB-Ctrl-ServerIronADX(config)#gslb-host-policy test
SLB-Ctrl-ServerIronADX(config-gslb-host-policy-test)#sticky
SLB-Ctrl-ServerIronADX(config)#gslb dns zone gslb.com
SLB-Ctrl-ServerIronADX(config-gslb-dns-gslb.com)#host-info www gslb-policy test
```

This example defines a host policy, then applies that policy to the specific host www. The **sticky** is one function within the host policy.

Syntax: [no] sticky

No special CLI commands need to be issued on the site ServerIron ADX.

Specifying sticky session prefix lengths

To create sticky for a specific group (subnet) of clients, configure a different prefix length for that group. Once configured, the GSLB controller will ensure that DNS clients within the same subnet will be served the same IP address in the GSLB response so long as the IP address belongs to the domain and is active.

By default, the ServerIron ADX creates sticky sessions for every IPv6 DNS client with a prefix length of 128 bits. The **ipv6-prefix-length** parameter enables you to specify an alternative prefix length.

To specify the prefix length, enter commands such as the following:

```
SLB-Ctrl-ServerIronADX(config)#gslb policy
SLB-Ctrl-ServerIronADX(config-gslb-policy)#sticky ipv6-prefix-length 64
```

Syntax: [no] **sticky ipv6-prefix-length** <*decimal* >

The **ipv6-prefix-length** parameter specifies the prefix length of IPv6 DNS clients. The parameter enables you to aggregate DNS clients into one sticky session. The default prefix length is 128 bits.

NOTE
ServerIron ADX does not support the synchronization of sticky sessions across BPs. With sticky ipv6-prefix-length configured, DNS requests from clients on the same subnet go to different BPs and different sticky sessions will be created on different BPs. However, each individual client will receive the same specific domain IP that it received in its previous DNS request.

Specifying sticky session life times

Sometimes clients do not accept DNS servers, thus creating stale sessions. The sticky GSLB session life time (age) prevents sessions from hanging for extended periods of time.

By default, the life time (age) of sticky sessions is set at five minutes. Use the **sticky age** command to specify the time (in minutes) that must past before an idle session “times out” and session resources are made available to other clients.

To configure the Sticky GSLB session life time (age), enter commands such as the following:

```
SLB-Ctrl-ServerIronADX(config)#gslb-host-policy test
SLB-Ctrl-ServerIronADX(config-gslb-host-policy-test)#stick age 5
```

Syntax: [no] **sticky age** <*value*>

The <*value*> is the number of minutes before sticky session is cleared.

Deleting sticky sessions

The **clear gslb ipv6 sticky-session** command enables you to clear all sticky sessions or sticky sessions for a specific client.

Syntax: **clear gslb ipv6 sticky-session** (**all** | <*client-ip*>)

The <*client-ip*> is the IP address or prefix of the client for which sticky session will be deleted. If the all option is used, the sticky sessions for all clients are cleared.

High availability considerations for IPv6 sticky persistence

Sticky GSLB enables the GSLB controller to return the same IP address if a client sends multiple DNS requests within a configurable period of time.

Controllers, when configured in HA scenarios, will need to sync their sticky sessions in order to maintain persistence across the controllers. This is similar to the IPV4 sticky persistence behavior.

IPV4 and IPV6 sticky sessions will share the same special signature. All sticky GSLB ipv6 sessions are identified by the client IP and the following three tuples that remain the same for all sticky sessions:

- Dst-IP - 255.0.255.0
- S-port – 7
- D-port – 8

```
ServerIronADX(config)# show session all 0
Session Info:
Flags - 0:UDP, 1:TCP, 2:IP, 3:INT, 4:INVD, H: sessInHash, N: sessInNextEntry
Index Src-IP           Dst-IP                                         S-port
D-port       Age          Next         Serv          Flags
===== ======          ======                                    ======      ======
===           ====         ====         ======
0    0.0.0.5           100.1.1.10                      5           80
0              000000      n/a           SLB1 H
1    0.0.0.5           100.1.1.30                      5           80
0              000000      n/a           SLB1 H
2     2001:0DB8::78  255.0.255.0                     7            8
57             000000      n/a          SLB3 H
3    100.1.1.0         255.0.255.0                     7            8
57             000000      n/a          SLB3 H
```

In the example, the second and third rows show IPV6 and IPV4 sticky sessions.

Hash-based persistence for IPv6

GSLB ServerIron ADX offers two methods for site persistence: sticky persistence and hash-based persistence.

Hash-based persistence is the best solution for site persistence in environments that utilize two GSLB controllers (not in an HA configuration) for the same domain and where site persistence is needed for a single client that is directed to those GSLB controllers. When users query for a host name, they receive the same IP address for that domain regardless of which GSLB controller is contacted.

Sticky persistence alone is sufficient for single-box and High Availability (hot standby, symmetric active-standby, symmetric active-active) topologies. For more information, see “Sticky persistence for IPv6” on page 222.

Specifying hash-based persistence prefix lengths

By default, the ServerIron ADX does hash-based GSLB persistence for every IPv6 DNS client with a prefix length of 128 bits. The **ipv6-prefix-len-hash-persist** parameter enables you to specify an alternative prefix length.

To create site persistence for a specific group (subnet) of clients, configure a different hash-based persistence prefix length for that group. Once configured, the GSLB controller will ensure that DNS clients within the same subnet will be served the same IP address in the GSLB response so long as the IP address belongs to the domain and is active.

To specify the prefix length, enter commands such as the following:

```
ServerIronADX(config)#gslb policy
ServerIronADX(config-gslb-policy)# ipv6-prefix-len-hash-persist 64
```

Syntax: [no] **ipv6-prefix-len-hash-persist** <*decimal* >

The **ipv6-prefix-len-hash-persist** parameter specifies the hash-based persistence prefix length of IPv6 DNS clients. The parameter enables you to aggregate DNS clients to go to one domain IP. The default prefix length is 128 bits.

Manually forcing a rehash for a domain

The **clear gslb ipv6 phash** command enables you to clear the hash tables related to IPv6 addresses.

To force a rehash of a persistent GSLB table, enter a command such as the following:

```
ServerIronADX# clear gslb ipv6 phash table all
```

Syntax: **clear gslb ipv6 phash table** [**all** | **zone-name** <*zone-name*> **host-name** <*host-name*>]

Use the c**lear gslb ipv6 phash counter** command to clear GSLB phash counters. For more information see “Clearing GSLB phash counters” on page 246.

Weighted hash-based persistence for IPv6

Weighted hash-based persistence allocates the hash buckets in a weighted round robin fashion, enabling you to not only maintain persistence, but also determine what percentage of the traffic goes to a particular domain IP address.

With weighted hash-based persistence, you can define hash weights for the IPs in a domain. The hash buckets are distributed among the domain IP addresses in proportion to these weights.

NOTE
All of the commands used to configure hash-based persistence IPv6 are also applicable to weighted hash based persistence.

Enabling weighted hash-based GSLB persistence

Weighted hash-based GSLB persistence can be enabled for all domains or for specific domains as needed. You can enable weighted hash-based persistence as the global or host-level policy. As a result, this feature applies to all the domains this policy is bound to.

NOTE
Weighted hash-based persistence cannot be enabled concurrently with sticky persistence in the same policy. However, you can enable sticky persistence for one policy and weighted hash-based persistence for another policy.

To enable weighted hash-based persistence globally, enter commands on the GSLB controller, such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# hash-persist  weighted
```

To enable weighted hash-based GSLB persistence for a host-level policy, enter commands on the GSLB controller, such as the following:

```
ServerIronADX# config t
ServerIronADX(config)# gslb-host-policy test
ServerIronADX(config-gslb-host-policy-test)# hash-persist  weighted
```

Syntax: [no] **hash-persist [weighted]**

NOTE
Note that **weighted** is an optional parameter. If "weighted" is not specified, then the old hash-based persistence mechanism will be in effect. The old hash-based persistence mechanism distributes the hash buckets in a round robin manner. If the mechanism is changed from hash-based persistence to weighted hash-based persistence or vice versa in a GSLB global or host-level policy, then the hash table for all domains associated with that policy will be rehashed.

GSLB hash-based persistence with configurable subnet mask length

ServerIron ADX allows specification of subnet mask while doing GSLB site persistence. The LB controller hashes the entire 32-bits of a LDNS IP address to generate the hash bucket for GSLB hash-based persistence. As a result, LDNS servers in the same subnet could be assigned to different hash buckets. We now provide a mechanism for the user to define a subnet length for hashing; only this portion of the LDNS IP address will be used to generate the hash bucket. As a result, user can ensure that all the LDNS servers that fall in the same subnet, as defined by the hash prefix length, will hash to the same bucket and be serviced by the same domain IP address. As an example, if the specified source subnet mask is /24 then all LDNS servers within a given /24 subnet would receive same response (site IP) from the GSLB controller.

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# prefix-len-hash-persist  24
```

Syntax: [no] **prefix-len-hash-persist** *<length>*

NOTE
This command should be configured under the GSLB global or host-level policy.

Configuring weights for domain IP addresses

Weighted hash-based persistence enables the user to distribute the hash buckets for the domain in proportion to the weights configured for the domain IP addresses. Use the following command line interface to configure weights for the domain IP addresses:

```
ServerIronADX(config)# gslb dns zone gslb.com
ServerIronADX(config-gslb-dns-gslb.com)# host www http
ServerIronADX(config-gslb-dns-gslb.com)# host www ip-hash-weight 2001:db8::10
ServerIronADX(config-gslb-dns-gslb.com)# host www ip-hash-weight 2001:db8::40
```

Syntax: **host-info** *<host-name>* **ip-hash-weight** *<IPaddress> <weight>*

- The *<host-name>* parameter specifies the host name.
- *<IP address>* is the IP address for which you are assigning a hash weight.

- <*weight*> is a value from 0 to 100. The default value is 1. A weight of 0 implies that the client IP will not be allocated any hash buckets. A weight of 0 can be used to designate a domain IP as backup.

NOTE
The aggregate of the hash weights for all the IPs for a domain does not have to add up to 100.

When user configures a hash weight of zero for a domain IP, no hash buckets are allocated to this domain IP. If the hash buckets for this domain does not have any other healthy IPs, then the best IP address among all the healthy IPs including the IP with hash weight of zero, will be selected based on the remaining GSLB metrics. So user can configure a domain IP to be used as a backup IP by configuring a weight of zero for this IP address.

Disabling rehash on introduction of new IP addresses or state change from down to healthy

You can disable rehash on the introduction of a new IP address or change of IP address state from down to healthy. Persistence that occurs when rehashing is performed is prevented. The trade-off is the new IP address will not be included in the hash table.

To disable rehash, enter commands such as the following:

```
SLB-ServerIronADX(config)# gslb policy
SLB-ServerIronADX(config-gslb-policy)# hash-persist persist-rehash-disable
```

Syntax: **hash-persist persist-rehash-disable** <*time-out*>

The <*time-out*> parameter specifies the number of seconds before an IP address is removed from the hash table when that IP becomes down. The default is five seconds.

Disabling rehash when weight for an IP is changed

When user changes the hash weight configured for an IP in the domain, GSLB controller will automatically rehash the hash table for that domain. You can disable this rehash on weight configuration change with the following command.

Use the following command line interface to disable rehashing on weight change for global GSLB policy:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# hash-persist disable-weight-rehash
```

Use the following command line interface to disable rehashing on weight change for host-level GSLB policy:

```
ServerIronADX# config t
ServerIronADX(config)# gslb-host-policy test
ServerIronADX(config-gslb-host-policy-test)# hash-persist disable-weight-rehash
```

Syntax: **[no] hash-persist disable-weight-rehash**

If the weight of an IP for a domain is changed and this command is configured, then a message, stating that the ServerIron ADX needs to be rehashed at a later time, will be displayed.

If user configures this command, he or she will have to manually rehash at a later convenient time. This command can be used when user does not want to break the persistence for the existing IP addresses due to a change in weight configuration. User will disable rehashing on weight configuration change to preserve persistence and instead will rehash manually at a later convenient time, such as during a maintenance window for the GSLB controller.

Hash persist hold down timer

Hash persist hold down timer is provided to handle the boot up case when rehash on state change from down to up or rehash on weight configuration change is disabled. This hold down timer specifies how long after boot up, the disabling of rehash on state or weight change takes effect. Any change to the configured hash weight will result in a rehash during the hold-down time (i.e. even if you have disabled rehash on weight change), it will become effective only after this hold-down time has elapsed.

After the GSLB ServerIron ADX boots up, it will perform a back-end query for the IP addresses associated with the domain. Once it obtains these addresses, the ServerIron ADX will determine their health. Therefore after boot up, the IPs may come up one after another instead of at the same time. The weights will get associated with the IPs as they come up; this means that even if rehash is disabled, a rehash must still be performed to handle this scenario.

To specify how long the disabling of rehash on weight change becomes effective after boot up, enter a command such as the following:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# hash-persist hold-down 5
```

Syntax: **hash-persist hold-down** <*time*>

Syntax: **[no] hash-persist hold-down** <*time*>

- The <*time*> parameter specifies the number of minutes (1-255) before rehash disable become effective after boot up.
- The default is five minutes.

NOTE
This command is provided in the existing hash-based persistence. The same command will be used for the weighted hash-based persistence as well.

Configuring DNS response parameters

Fragmentation is not supported for the GSLB ServerIron ADX for IPv6.

Therefore, you must either configure an active-only policy or best-only policy or ensure that the number of IP addresses configured in the IP list is small enough to avoid fragmentation

Configuring an active-only policy

By default, the ServerIron ADX does not remove an IP address from a DNS reply even if the address fails a health check.

You can configure the ServerIron ADX to remove IP addresses from DNS replies when those addresses fail a health check. The ServerIron ADX removes the addresses that fail the check so long as the DNS query still contains at least one address that passes the health check.

A site must pass all applicable Layer 4 and Layer 7 health checks to avoid being removed.

NOTE
If all the sites fail their health checks, resulting in all the sites being rejected by the GSLB ServerIron ADX, the ServerIron ADX sends the DNS reply unchanged to the client.

The GSLB default behavior is as follows:

- In DNS proxy, the entire list of IP addresses is sent back to the client with the best IP address selected by the GSLB controller at the top of the list. This best IP is selected in accordance with the GSLB policy. An administrator typically configures an active-only policy, because the LDNS may cache this response for TTL time and may round robin the IPs in this list in some cases.
- Health check in the GSLB policy is disabled. Typically administrators will not disable health check if they are using an active-only policy.
- An active-only policy applies only to the remaining IP addresses in the IP list, not the best one. An administrator should enable health check for best IP selection to ensure that best IP is healthy.

To configure the ServerIron ADX to remove IP addresses from DNS replies when those addresses fail a health check, enter the following commands:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns active-only
```

Syntax: [no] dns active-only

Configuring a best-only policy

The GSLB policy places the best IP address selected by the GSLB policy at the top of the list.

Use the **dns best-only** command to configure the ServerIron ADX to return only the best IP address in the DNS response.

NOTE
If the GSLB policy does not result in the selection of a “best” address, the DNS reply can still contain multiple addresses.

To configure the GSLB ServerIron ADX to remove all addresses except the best address from the DNS replies, enter the following commands:

```
ServerIronADX(config)# gslb policy
ServerIronADX(config-gslb-policy)# dns best-only
```

Syntax: [no] dns best-only

GSLB of ANY queries

DNS supports many different record types including IPv4 address records (A records), IPv6 address records (AAAA records), Name Server records (NS records), Mail Exchange (MX records), Canonical Name records (CNAME records) and so on. DNS also supports a special query type called "ANY".

If a client sends an ANY query, the GSLB ServerIron ADX applies the GSLB policy to the IP addresses configured for that domain in its IP list.

- If the host has an IPv6 IP list configured, the ServerIron ADX applies GSLB policy to the addresses on the list and responds with AAAA records.
- If the host has an IPv4 IP list configured, the ServerIron ADX applies GSLB policy to the addresses on the list and responds with A records.
- If the host has both IPv6 and IPv4 IP lists configured, the ServerIron ADX applies GSLB policy to the addresses on both the lists and responds with both AAAA and A records.

Displaying GSLB for IPv6 configurations

Show commands enable you to view key information about the ServerIron ADX components, configurations, and policies.

Table 21 lists key show commands for basic and advanced ServerIron ADX configurations.

TABLE 21 GSLB for IPv6 show commands

Feature	See page...
Basic configuration	
Displaying GSLB global statistics	page 231
Displaying default GSLB policy	page 232
Displaying the user-configured policy	page 234
Displaying information about geographic prefixes	page 235
Displaying DNS zones	page 237
Displaying detailed DNS information	page 241
Displaying sites	page 245
Advanced configuration	
Displaying the hash table	page 245
Clearing GSLB hash counters	page 246

Show commands for basic GSLB configurations

Displaying DNS cache proxy statistics

Use the **show gslb global-stat** command, to see view information about the number and type of DNS queries the GSLB ServerIron ADX has responded to.

NOTE
The counter displayed from the **show gslb global-stat** command are maintained differently on the management and BP consoles. On the management console the counts are aggregated from all BPs. On the BP console the count displayed os only for the BP being accessed.

To display DNS cache proxy statistics, enter the command **show gslb global-stat** at any level of the CLI.

```
show gslb global-stat
DNS cache proxy stat:
```

```
Direct response      =          0 Query type ANY       =          0
Query type A         =         56 Query type AAAA      = 87
```

The command returns information about the number of requests for three query types: queries for IPv4 addresses (A records), queries for IPv6 addresses (AAAA records), and ANY queries. The Direct Response field shows the total number of DNS queries that the GSLB ServerIron ADX has responded to directly.

Syntax: **show gslb global-stat**

Displaying the default GSLB policy

Use the **show gslb default** command to view the default GSLB policy settings for the ServerIron ADX including the default processing order of the GSLB policy algorithm and the status of many optional features including the active-only and best-only DNS response parameters.

To display the default GSLB policy, enter the **show gslb default** command:

```
ServerIronADX(config)# show gslb default
  Default metric order: ENABLE
  Metric processing order:
                1-Server health check
                2-Remote ServerIronADX's session capacity threshold
                3-Round trip time between remote ServerIronADX and client
                4-Geographic location
                5-Remote ServerIronADX's available session capacity
                6-Server flashback speed
                7-Least response selection

  DNS active-only: DISABLE   DNS best-only: DISABLE   DNS override: DISABLE
  Modify DNS response TTL: ENABLE
  DNS TTL: 10 (sec), DNS check interval: 30 (sec)
  Remote ServerIronADX status update period: 30 (sec)
  Session capacity threshold: 90%, session capacity tolerance: 10%
  Round trip time tolerance: 10%, round trip time explore percentage: 5%
  Round trip time cache prefix: 20, round trip time cache interval: 120 (sec)
  Flashback appl-level delay tolerance: 10%, TCP-level delay tolerance: 10%
```

Syntax: **show gslb default**

This display shows the following information.

TABLE 22 GSLB policy information

This field...	Displays...
Default algorithm	Indicates whether this policy is in effect. The value can be one of the following: • Disable • Enable If the state is Disable, then a user-configured policy is in effect instead.
Metric processing order	Indicates the order in which the selection metrics are applied to the server addresses in the DNS reply.

TABLE 22 GSLB policy information (Continued)

This field...	Displays...
DNS active-only	Indicates whether the GSLB ServerIron ADX removes IP addresses from the DNS response if those addresses fail a health check. This field can have one of the following values: • **DISABLE**: The ServerIron ADX does not remove the IP addresses from the DNS response. • **ENABLE**: The ServerIron ADX removes IP addresses that fail a health check from the DNS response.
DNS best-only	Indicates whether you have configured the ServerIron ADX to remove all IP addresses except the "best" address from DNS replies. This field can have one of the following values: • **DISABLE**: The ServerIron ADX does not remove all addresses except the best one. • **ENABLE**: The ServerIron ADX removes all addresses except the best one. **NOTE:** Even when this feature is enabled, if the GSLB policy does not result in selection of a best address, the DNS reply can still contain more than one address. For more information, refer to "Configuring a best-only policy" on page 230.
DNS override	Indicates whether DNS override is enabled. DNS override replaces the addresses in a DNS reply with the "best" address from a list of addresses you configure. This field can have one of the following values: • **DISABLE**: The ServerIron ADX does not replace the addresses in DNS replies with an address from a list you configure. • **ENABLE**: The ServerIron ADX replaces the addresses in DNS replies with an address from a list you configure. For more information about DNS override, refer to "Enabling DNS override" on page 198.
Modify DNS response TTL	Indicates whether the GSLB ServerIron ADX modifies the TTL in the DNS records in DNS responses before sending the responses to the client's DNS server. This field can have one of the following values: • **DISABLE**: The ServerIron ADX does not modify the TTLs. • **ENABLE**: The ServerIron ADX modifies the TTLs.
DNS TTL	Indicates the value (number of seconds) to which the GSLB ServerIron ADX changes the TTL in each DNS record in the DNS responses before sending them to the client's DNS server. **NOTE:** If the Modify DNS response TTL field contains "DISABLE", the ServerIron ADX does not change the TTLs, regardless of the value in this field.
DNS check interval	Indicates how frequently the GSLB ServerIron ADX refreshes its zone and host information with DNS servers.
Remote ServerIron ADX status update period	Indicates how frequently the remote ServerIron ADXs send status updates to the GSLB ServerIron ADX through the GSLB protocol.
Session capacity threshold	Specifies how close to its maximum session capacity the site ServerIron ADX (remote ServerIron ADX) can be and still be eligible as the best site for the client. If a site ServerIron ADX exceeds the threshold, the site ServerIron ADX is ineligible to be the best site.
Session capacity tolerance	Specifies the percentage by which the number of available sessions on the site ServerIron ADX can differ from the number of available sessions on another site ServerIron ADX and still be considered an equally good site.

TABLE 22 GSLB policy information (Continued)

This field...	Displays...
Round trip time tolerance	Specifies the percentage by which the RTT for one site can differ from the RTT for another site without this metric resulting in selection of one site over the other.
Round trip time explore percentage	Indicates the percentage of client requests from a given network for which the GSLB ServerIron ADX intentionally ignores the RTT metric when evaluating the IP addresses in the DNS reply. The explore percentage prevents the ServerIron ADX from continually biasing its site selection based on the first ServerIron ADX to return RTT information. Refer to "Modifying round-trip time values" on page 53.
Round trip time cache prefix	Indicates the length (number of significant bits) of entries in the GSLB ServerIron ADX's IP address cache. The prefix determines the extent to which IP addresses are aggregated into entries in the cache.
Round trip time cache interval	Indicates how many seconds the GSLB ServerIron ADX keeps an unrefreshed RTT cache entry in its cache before the entry ages out.
Flashback appl-level delay tolerance	Indicates the percentage of difference that can exist between application level FlashBack response times for two sites, without the ServerIron ADX preferring one site over the other based on this metric.
TCP-level delay tolerance	Indicates the percentage of difference that can exist between Layer 4 FlashBack response times for two sites, without the ServerIron ADX preferring one site over the other based on this metric.

Displaying the user-configured GSLB policy

Use the **show gslb policy** command to view user-defined GSLB policy settings for the ServerIron ADX including the default processing order of the GSLB policy algorithm and the status of many optional features including the active-only and best-only DNS response parameters.

To display the user-configured GSLB policy, enter the following command.

```
ServerIronADX(config)# show gslb policy
  Default metric order: ENABLE
  Metric processing order:
                1-Server health check
                2-Remote ServerIronADX's session capacity threshold
                3-Round trip time between remote ServerIronADX and client
                4-Geographic location
                5-Remote ServerIronADX's available session capacity
                6-Server flashback speed
                7-Least response selection

  DNS active-only: DISABLE   DNS best-only: DISABLE   DNS override: DISABLE
  Modify DNS response TTL: ENABLE
  DNS TTL: 10 (sec), DNS check interval: 30 (sec)
  Remote ServerIronADX status update period: 30 (sec)
  Session capacity threshold: 90%, session capacity tolerance: 10%
  Round trip time tolerance: 10%, round trip time explore percentage: 5%
  Round trip time cache prefix: 20, round trip time cache interval: 120 (sec)
  Flashback appl-level delay tolerance: 10%, TCP-level delay tolerance: 10%
```

In this example, the default order of the policy metrics is in effect. Metrics that are disabled by default (such as the administrative preference) are not listed.

In the following example, the order has been changed, two of the metrics have been disabled, and the administrative preference has been enabled.

```
ServerIronADX(config)# show gslb policy
  Default metric order: DISABLE
  Metric processing order:
                1-Round trip time between remote ServerIronADX and client
                2-Remote ServerIronADX's session capacity threshold
                3-Remote ServerIronADX's available session capacity
                4-Server flashback speed
                5-Remote ServerIronADX's preference value
                6-Least response selection

  DNS active-only: DISABLE   DNS best-only: DISABLE   DNS override: DISABLE
  Modify DNS response TTL: ENABLE
  DNS TTL: 10 (sec), DNS check interval: 30 (sec)
  Remote ServerIronADX status update period: 30 (sec)
  Session capacity threshold: 90%, session capacity tolerance: 10%
  Round trip time tolerance: 10%, round trip time explore percentage: 5%
  Round trip time cache prefix: 20, round trip time cache interval: 120 (sec)
  Flashback appl-level delay tolerance: 10%, TCP-level delay tolerance: 10%
```

For a description of the information shown by this command, refer to “Displaying the default GSLB policy” on page 232.

Syntax: **show gslb policy**

Displaying information about a geographic prefix

To view information about a specific geographic prefix, enter the following command on the GSLB ServerIron ADX:

```
GSLB-ServerIronADX# show gslb ipv6 cache 2001:db8::
prefix length = 64, prefix = 2001:db8::, region = N-AM
prefix source = geographic (static),
```

Syntax: **show gslb ipv6 cache [geographic (user-configured | static)]**

The **static** option returns only those entries which were created internally by GSLB ServerIron ADX. The **user-configured** option returns entries created by the user using the **geo-prefix** command.

Displaying results of traffic distribution for weighted sites

Use the **show gslb traffic site** command to view information about the domains hosted by each site. For each domain name, the command shows that amount of traffic that was sent to each ServerIron ADX in that site, and the total percentage of traffic sent to the site.

To view the results of traffic distribution after configuring weighted site metrics, enter the following command:

```
ServerIronADX(config)# show gslb traffic site

SITE: local                             Weight: 50
        * a.b.c
          DNS Requests: 36
                ServerIronADX VIP                 Selection (%)
                  ==               ===               =============
                  2001:db8::1      2001:db8::181     9 (25 %)
                  2001:db8::1      2001:db8::180     9 (25 %)
          Site Selection for Domain: 18 (50 %)
        * b.b.c
          DNS Requests: 0
                ServerIronADX VIP                 Selection (%)
                  ==               ===               =============
                  2001:db8::1      2001:db8::121     0 (0 %)
          Site Selection for Domain: 0 (0 %)

SITE: TWO                               Weight: 50
        * a.b.c
          DNS Requests: 36
                ServerIronADX VIP                 Selection (%)
                  ==               ===                 =============
                  2001:db8::2      2001:db8::182           18 (50 %)
          Site Selection for Domain: 18 (50 %)
        * b.b.c
          DNS Requests: 0
                ServerIronADX VIP                 Selection (%)
                  ==               ===                 =============
                  2001:db8::2      2001:db8::122           0 (0 %)
          Site Selection for Domain: 0 (0 %)
```

The first example shows the first two sites.

The second example shows the third site.

```
SITE: THREE

        * a.b.c
          DNS Requests: 36

                ServerIronADX VIP                 Selection (%)
                  ==               ===                 =============
                  2001:db8::3      2001:db8::183           0 (0 %)
          Site Selection for Domain: 0 (0 %)

        * b.b.c
          DNS Requests: 0

                ServerIronADX VIP                 Selection (%)
                  ==               ===                 =============
                  2001:db8::3      2001:db8::123           0 (0 %)
          Site Selection for Domain: 0 (0 %)
```

In the above examples, there are two hosts; a (HTTP) and b (FTP) which belong to the zone b.c. There are three sites as listed below:

- Local (weight: 50; ServerIron ADX: 2001:db8::1; VIPs: 2001:db8::180 (HTTP), 2001:db8::181 (HTTP), 2001:db8::121 (FTP)
- TWO (weight: 50; ServerIron ADX: 2001:db8::2; VIPs: 2001:db8::182 (HTTP), 2001:db8::122 (FTP))
- THREE (weight: 0; ServerIron ADX: 2001:db8::3; VIPs: 2001:db8::183 (HTTP), 2001:db8::123 (FTP))

The IP resolution for the domain names is as follows:

- a.b.c.: 2001:db8::180; 2001:db8::181; 2001:db8::182
- b.b.c.: 2001:db8::121; 2001:db8::1.122

After making 36 requests for domain "a.b.c.", the distribution was:

- Site Local got 18 requests (VIP 2001:db8::180 received 9 and VIP 2001:db8::181 received 9)
- Site TWO got 18 requests (VIP 2001:db8::182 received all 18)

Site THREE did not receive any requests because its weight is zero.

Syntax: **show gslb traffic site**

Displaying DNS zone and hosts

Use the **show gslb dns** command to view information about the DNS zones and host names on GSLB controllers. The command can be used with or without the <*zone-name*> variable, which specifies a single zone. If this variable is omitted, all zones are displayed.

NOTE
If you also want to display information about the site and ServerIron ADX on which a VIP is configured, use the **show gslb dns detail** command instead. Refer to “Displaying detailed DNS information” on page 241.

To display GSLB information about a specific DNS zone, you must specify the zone such as in the example:

```
ServerIronADX(config)# show gslb dns zone brocade.com

ZONE: brocade.com
HOST: www:
(Global GSLB policy)
GSLB affinity group: global
                                                    Flashback  DNS resp.
                                                    delay      selection
                                                    (x100us)   counters
                                                    TCP  APP   Count(%)
* 10.18.2.155:    cfg    v-ip       ACTIVE N-AM.      0  0      1 (33%)
* 10.18.2.166:    cfg    v-ip       ACTIVE N-AM.      0  0      1 (33%)
* 2001:db8::1:    cfg    v-ip       ACTIVE N-AM.      0  0      1 (33%)
* 2001:db8::5:    cfg    real-ip    DOWN   N-AM.      --  --    0 (0%)
```

The information displayed is the same as that when you do not specify a zone name, except the zone field is unneeded and thus does not appear.

Syntax: **show gslb dns zone** [<*zone-name*>]

The <*zone-name*> parameter specifies the name of the zone to be displayed.

Output differs depending on the ServerIron ADX device used and the software release installed on the ServerIron ADX.

TABLE 23 GSLB zone and host application information

This field...	Displays...
ZONE	The zone name. The name that appears here is the name you specified when you configured the zone information. **NOTE:** This field appears only if you do not specify the zone name when you display the information. If you specify the zone name, information for only that zone is displayed.
HOST	The host name. The name that appears here is the name you specified when you configured the host information.
IP addresses	The column of IP addresses lists the IP addresses the authoritative DNS server associated with the host name in the DNS reply. These are the servers that contain the content for the host. In this example, the servers contain the content for www.brocade. After evaluating the addresses using the GSLB policy, the GSLB ServerIron ADX marks each address that passes the algorithm with an asterisk (*). An IP address that does not have an asterisk in front of it has not passed the GSLB algorithm and cannot be selected as the “best” site. **NOTE:** If DNS override is enabled, only the addresses configured in the host’s IP list have asterisks and are valid choices for the best site. Refer to “Enabling DNS override” on page 198.
Source	The value following each server IP address indicates how the ServerIron ADX learned the address. This field can have one of the following values: • **cfg**: The address is one that you associated with the host as part of the DNS override feature. Refer to “Enabling DNS override” on page 198. • **d/c**: The address was learned from the DNS server and also is one that you associated with the host. • **dns**: The address was learned from the DNS server. In the example above, the ServerIron ADX learned about all the IP addresses associated with the zone name from the IP list; thus, the source is listed as “cfg”.
Type	The next value indicates the type of address, which can be one of the following: • **v-ip**: The address is a VIP configured on a ServerIron ADX. • **real-ip**: The address is a real server.

TABLE 23 GSLB zone and host application information (Continued)

This field...	Displays...
State	The state of the server. The ServerIron ADX determines the state based on the results of the Layer 7 health checks sent to the server. The ServerIron ADX sends Layer 7 health checks for each host application you associate with the zone. The state can be one of the following: • ACTIVE: The server passed the Layer 4 and Layer 7 health checks and is presumed to be available. • DOWN: The server failed a health check. If any of the health checks are failed, the GSLB ServerIron ADX disqualifies this site from being the “best” site. NOTE: If the server has multiple applications, all the applications must pass the health check. NOTE: The ServerIron ADX also uses the results of the health check, if the server passes the check, in the TCP and App columns under FlashBack Delay, described below.
Location	The geographic location of the server. The location is based on the IP address and can be one of the following: • ASIA • EUROPE • N-AM: North America • S-AM: South America • AFRICA The GSLB ServerIron ADX can use this information when comparing the servers in order to select the “best” ones for the client. The GSLB ServerIron ADX prefers servers within the client’s geographic region over servers in other geographic regions.
FlashBack Delay (x100us)	The round-trip time for a health check sent by the GSLB ServerIron ADX to the host application on the server. The GSLB ServerIron ADX can use this information when comparing the servers in order to select the “best” ones for the client. The GSLB ServerIron ADX prefers servers with lower round-trip times to those with higher round-trip times. The value in the TCP column indicates the round-trip time of the Layer 4 health check to the TCP port. The value in the App column indicates the round-trip time for the Layer 7 health check. NOTE: A single value is displayed even if the zone has multiple host applications. If the FlashBack values (round-trip times) differ, the slowest times are displayed.
DNS resp. selection counters Count	The number of times the GSLB ServerIron ADX has selected this server as the “best” server and thus placed the server’s IP address at the top of the list in DNS replies.
DNS resp. selection percentage (%)	The percentage of times the GSLB ServerIron ADX has selected this server as the “best” server and thus placed the server’s IP address at the top of the list in DNS replies.

Use the **show gslb dns** command to view information about the distribution of traffic after the configuration of weighted IP metrics.

The command can be used with or without the <*zone-name*> variable, which specifies a single zone. If this variable is omitted, all zones are displayed.

```
ServerIronADX(config)# show gslb dns zone brocade.com

ZONE: brocade.com
HOST: www:
(Global GSLB policy)
GSLB affinity group: global
                                                    Flashback  DNS resp.
                                                    delay      selection
                                                    (x100us)   counters
                                                    TCP  APP   Count(%)
* 2001:db8::abc:  cfg    v-ip        ACTIVE N-AM.      0   0     1 (33%)
* 2001:db8::def:  cfg    v-ip        ACTIVE N-AM.      0   0     1 (33%)
* 2001:db8::1:    cfg    v-ip        ACTIVE N-AM.      0   0     1 (33%)
* 2001:db8::5:    cfg    real-ip     DOWN   N-AM.      --  --    0 (0%)
```

In the example above, the GSLB controller learned about all the IP addresses associated with the zone brocade.com from the IP list; thus, the source for each is listed as “cfg”. Traffic has been evenly distributed across the three active IP addresses.

Clearing DNS selection counters

The GSLB ServerIron ADX maintains DNS selection statistics for each IP address based on DNS requests served for a particular domain name. These DNS selection statistics include:

- How many times the IP address was selected as the best IP address
- Which metrics were used for making the IP address selection
- The percentage of times an IP address was selected in comparison with other IP addresses in the same domain name

Use the **show gslb dns zone** command to display the DNS selection statistics.

DNS selection statistics are used to implement GSLB metrics such as least response, weighted site and weighted IP metrics. Each of these metrics base subsequent selections on the number of times the IP address was previously selected. For example, the weighted site metric selects the IP address that has the least relative weight, the calculation of which is based on the selection counter of that IP address.

It can be advantageous to use the clear DNS selection counters feature in conjunction with GSLB metrics. Consider the following examples:

- The least response selection metric selects the IP address that has been selected the least number of times when compared to other IP addresses. If an IP address has become available after having been down for some time, it might suddenly become flooded with subsequent traffic because its selection counter is low. Clearing the counters for that zone can prevent a flood to this IP address.
- You can also use this feature to test the GSLB implementation before deploying it on a wider scale. You can analyze the effectiveness of each GSLB metric by rearranging the metric order and using the Clear Counters feature to start over without having to reload the software.

To clear DNS selection counters globally or per zone, without reloading the software, or to clear out any DNS requests for any client, enter a command such as the following:

```
ServerIronADX# clear gslb dns zone zone1
```

Syntax: **clear gslb dns zone-name** [<*name*>]

Replace <*zone-name*> with the zone for which you want to clear the DNS selection counters. To clear the counters globally (for all zones), do not enter a <*zone-name*>.

Displaying detailed DNS information

Use the **show gslb dns detail** command to view detailed information about the DNS zones and host names on GSLB controllers. Using this command, you can view key information about a zone including its IP list and selection criteria as well as information about the site and ServerIron ADX on which a VIP is configured.

The command can be used with or without the <*zone-name*> variable, which specifies a single zone. If this variable is omitted, all zones are displayed.

To display detailed GSLB information about a specific DNS zone, you must specify the zone such as in the example:

```
ServerIronADX# show gslb dns detail brocade.com

ZONE: brocade.com
HOST: www
(Global GSLB policy)
GSLB affinity group: global
                                             Flashback    DNS resp.
                                             delay        selection
                                             (x100us)     counters
                                             TCP  APP     Count (%)

*    10.18.2.155:  cfg   v-ip   ACTIVE  N-AM   0     0     1 (33%)
                   Active Bindings: 1
                   site: A, weight: 0, SI: name (10.18.2.150)
                   session util:   0%, avail. sessions: 3999980
                   preference: 128
                   Metric counter (count [selection-metric]):
                   1 [least-response]

*    2001:db8::a:  cfg   v-ip   ACTIVE  N-AM   0     0     1 (33%)
                   Active Bindings: 0
                   site: B, weight: 0, SI: name (10.18.2.160)
                   session util:   0%, avail. sessions: 5999985
                   preference: 128
                   Metric counter (count [selection-metric]):
                   1 [least-response]

*    10.18.25.23:  cfg   real-ip ACTIVE N-AM   470   1093  1 (33%)
*    2001:db8::1:  cfg   real-ip DOWN   N-AM   ---   ---   0 (0%)
```

Syntax: **show gslb dns detail** [<*zone-name*>]

The <*zone-name*> parameter specifies a particular GSLB zone.

TABLE 24 Global SLB zone and host application information

This field...	Displays...
Active bindings	Active bindings are a measure of the number of active real servers bound to a Virtual IP address (VIP) residing on a GSLB site. The GSLB ServerIron ADX uses the active bindings metric to select the best IP address for the client. The VIP with the highest number of active bindings is the IP address preferred by the active bindings metric
Site	Indicates the site name of the ServerIron ADX.
Weight	The weight assigned to the address for the weighted IP metric. Refer to "Specifying the weight of IP addresses in the IP list" on page 210.
Si Name	Indicates the site ServerIron ADX name and management IP address.
Session util	Indicates the percentage of the ServerIron ADX session capacity that is in use. This information is reported by the site ServerIron ADX using the GSLB protocol.
Avail. sessions	Indicates the number of unused sessions in the ServerIron ADX's session table.
Preference	The numeric preference value for this site ServerIron ADX. The preference can be used by the GSLB policy to select a site. Refer to "Site ServerIron ADX's administrative preference" on page 11.
Metric counter	The metric statistics are displayed under the Metric counter line. In this example, sites 10.18.2.15 and 2001:db8::a have each been selected as the best site once. This is shown in the DNS resp. selection counters column. The least response metric was used once to select each site.

For descriptions of the other information displayed by the **show gslb dns detail** command, refer to "Displaying DNS zone and hosts" on page 237.

Displaying site information

Use the **show gslb site** command to display the following information about sites:

- ServerIron ADX name and management IP address
- Site name (displayed only if you display information for all sites rather than an individual site)
- State of the GSLB protocol connection between GSLB ServerIron ADX and site ServerIron ADX
- Number of sessions in the ServerIron ADX's session table
- The percentage of the total number of sessions the ServerIron ADX can maintain that are in use
- The percentage of the ServerIron ADX's CPU that is actively engaged in SLB and other activities
- The numeric preference value for this site ServerIron ADX
- The geographic location of the ServerIron ADX
- The virtual IP addresses (VIPs) configured on the ServerIron ADX

The **show gslb site** command can be used with or without the <*site-name*> variable, which specifies a single site. If this variable is omitted, all sites are displayed.

To display information for all configured sites, enter the following command at any level of the CLI:

```
ServerIronADX(config)# show gslb site
SITE: sunnyvale
ServerIronADX: slb-1 209.157.22.209:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
       500000       50         35  128         N-AM
 Virtual IPs:
     209.157.22.227(A)         209.157.22.103(A)
ServerIronADX: slb-2 209.157.22.210:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
            1        0         16  128         N-AM
 Virtual IPs:
     209.157.22.227(S)
SITE: atlanta
ServerIronADX: slb-1 192.108.22.111:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
       750000       75         41  128         N-AM
 Virtual IPs:
    209.157.22.227(A)          209.157.22.104(A)
ServerIronADX: slb-1 192.108.22.111:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
            1       0         16   128         N-AM
 Virtual IPs:
    209.157.22.227(S)
```

To display information about a specific GSLB site and the ServerIron ADXs providing SLB within that sites, identify the site using its site name. For example, to view information about a GSLB site called “Sunnyvale”, enter the following command:

```
ServerIronADX(config)# show gslb site sunnyvale
ServerIronADX: slb-1 209.157.22.209:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
       500000       50         35  128         N-AM
 Virtual IPs:
     209.157.22.227(A)
ServerIronADX: slb-2 209.157.22.210:
state: CONNECTION ESTABLISHED
 Current num.  Session   CPU load  Preference  Location
 sessions      util(%)   (%)
            1        0         16  128         N-AM
 Virtual IPs:
     209.157.22.227(S)
```

The **show gslb site sunnyvale** command returns the following information:

TABLE 25 **Global SLB site information**

This field...	Displays...
ServerIron ADX name and IP address	For each ServerIron ADX, the first item of information listed is the name and management IP address. This is the information you specified when you added the ServerIron ADX to the site.
SITE	Indicates the site name of the ServerIron ADX. NOTE: This field appears only when you enter the **show gslb site** command without specifying a site name.
ServerIron ADX	Indicates the site ServerIron ADX name and management IP address.
State	The state of the GSLB protocol connection between the GSLB ServerIron ADX and the site ServerIron ADX. The state can be one of the following: • ATTEMPTING CONNECTION: The GSLB ServerIron ADX is still trying to establish a GSLB connection with the site ServerIron ADX. • CONNECTION ESTABLISHED: The GSLB ServerIron ADX has established a GSLB connection with the site ServerIron ADX. • SELF: The GSLB ServerIron ADX is also this site ServerIron ADX.
Current num. sessions	The number of sessions in the ServerIron ADX's session table. A session is a one-way connection to or from a real server. This information is reported by the site ServerIron ADX. NOTE: The number of sessions in the table does not necessarily match the number of active sessions on the real servers. This can occur if the session table contains sessions that are no longer active but have not yet timed out.
Session util (%)	The percentage of available sessions that are in use. This is the percentage of the total number of sessions the ServerIron ADX can maintain that are in use. For example, if the ServerIron ADX can maintain 1 million sessions (the default session capacity) and the session table contains 500,000 session entries, the session utilization is 50%. This information is reported by the site ServerIron ADX.
CPU load (%)	The percentage of the ServerIron ADX's CPU that is actively engaged in SLB and other activities. This information is reported by the site ServerIron ADX.
Preference	The numeric preference value for this site ServerIron ADX. The preference can be used by the GSLB policy to select a site. Refer to "Administrative preference metric" on page 220. This information is configured on the GSLB ServerIron ADX.

TABLE 25 Global SLB site information (Continued)

This field...	Displays...
Location	The geographic location of the ServerIron ADX. The location is based on the ServerIron ADX’s management IP address and can be one of the following: • ASIA • EUROPE • N-AM: North America • S-AM: South America • AFRICA **NOTE:** If you explicitly identified the geographic location, the value you specified appears instead of a value based on the IP address. Refer to “Configuring sites” on page 200.
Virtual IPs	The virtual IP addresses (VIPs) configured on the ServerIron ADX. This information is reported by the site ServerIron ADX. The letter in parentheses at the end of each address indicates whether the ServerIron ADX is an active or standby ServerIron ADX for that address. The letter can be A (active) or S (standby). Unless the ServerIron ADX is configured along with a partner ServerIron ADX for Symmetric Server Load Balancing, the value is always A. If a number appears following the A or S, a host range (the unlimited VIP feature) is configured on the VIP. The number indicates the number of hosts in the host range. **NOTE:** The GSLB ServerIron ADX does not necessarily provide global SLB for all the VIPs configured on the site ServerIron ADXs. The GSLB provides global SLB only for the VIPs that correspond to the DNS zone names you configure the GSLB ServerIron ADX to load balance.

Syntax: **show gslb site** [<*site-name*>]

The <*site-name*> parameter specifies a site name.

Show commands for advanced features

Displaying the hash table

A hash table is maintained for a domain for which hash-based persistence is enabled in the associated policy. There are 256 entries in the hash table, and there is a domain IP address associated with each of these entries.

Use the **show gslb ipv6 phash** command to view the status of the IPv6 hash table.

To display the hash table for all domains or a specific zone, enter a command such as the following:

```
ServerIronADX# show gslb ipv6 phash table all

Persistent Hash table for www.lokdom.com
number of active IP:1
number of IP used for hashing: 1
rehash is disabled: FALSE
rehash on weight change is disabled: FALSE
hash prefix length: 128
bucket 0: ipv6 2001:db8::150, hit count 0
bucket 1: ipv6 2001:db8::150, hit count 0
bucket 2: ipv6 2001:db8::150, hit count 0
bucket 3: ipv6 2001:db8::150, hit count 0
```

Syntax: **show gslb ipv6 phash (active-ip | allocation | table)**

The optional **active-ip | allocation | table** parameter specifies the information that you want to see.

- The **table** operand displays the persistent GSLB hash table.
- The **active-ip** operand shows the current active IP address.
- The **allocation** operand shows the hash bucket for the client IP.

Clearing GSLB phash counters

Syntax: **clear gslb ipv6 phash counter** [**all** | **zone-name** <*name*> **host-name** <*name*>]

Troubleshooting GSLB for IPv6 configurations

The commands discussed in this section enable you to troubleshoot ServerIron ADX configurations.

Table 26 lists key troubleshooting commands.

TABLE 26 GSLB for IPv6 troubleshooting commands

Feature	See page...
Displaying GSLB debug counters	page 246
Troubleshooting IPv6 IP lists	page 248
Debug trace for GSLB	page 248

Displaying GSLB debug counters

The **show gslb debug-counter** command enables you view information that can enable you to debug a GSLB configuration.

To view show GSLB debug information and error statistics, run the following command:

```
ServerIronADX 1000(config)#show gslb debug-counter
GSLB debug counter can not find peerTcpP when connection close: 9
GSLB debug counter 122: 261079

*********************************************
Error stats:
Num valid SI vip deletion error: 0
Num VIP SI record deletion error: 0

*********************************************
Domain IP creation stats for BP:
Num domain IPs added sync table: 33

*********************************************
PAX Mem domain IP debug information:
***********************************************
Num MP domain IP config pax mem alloc: 71
Num MP domain IP non-config pax mem alloc: 0
Num MP domain IP pax mem delete: 36
```

```
*********************************************
PAX Mem dynamic real virtual debug information:
***********************************************
Num MP dyn VIP pax mem alloc: 255466
Num MP dyn VIP pax mem alloc del err: 0
Num MP dyn VIP pax mem delete: 255462
Num MP dyn VIP port pax mem alloc: 255466
Num MP dyn VIP port pax mem delete: 255462
Num MP dyn real svr pax mem alloc: 305324
Num MP dyn real svr pax mem alloc del error: 0
Num MP dyn real svr pax mem delete: 305310
Num MP dyn real port pax mem alloc: 305370
Num MP dyn real port pax mem delete: 305352


*********************************************
Phash memory debug information:
***********************************************
Num phash new IP mem alloc: 16
Num update IPv4 alloc mem alloc: 5
Num update IPv6 alloc delete: 12
Num phash host mem alloc: 0
Num phash zone mem alloc mem alloc: 0
Num phash all mem alloc: 0

*********************************************
Dynamic memory stats:
***********************************************
VIP port hcheck alloc:
gslb_debug_vip_port_malloc_mem: 8966153
gslb_debug_vip_port_malloc_update_si_vip: 0
gslb_debug_vip_port_malloc_update_si_vip_with_hashing_ts: 18519513
gslb_debug_vip_port_malloc_update_si_vip_with_hashing: 417636
gslb_debug_vip_port_mem_free: 3967960
gslb_debug_vip_port_mem_ts_free: 1983942
gslb_debug_delete_vip_num_free_vip_port_list: 3014192
gslb_debug_delete_vip_num_free_vip_port_list_ts: 419446
gslb_debug_vip_port_free_update_si_vip_with_hashing_ts: 18517276
gslb_stale_vip_list_cnt: 0

gslb sticky:
gslb_debug_sticky_dyn_mem_alloc: 0

domain url web:
gslb_debug_option_http_url_mem_alloc_web: 0
gslb_debug_option_http_url_mem_alloc_url: 0
gslb_debug_sptr_web_url_free: 0
gslb_debug_sptr_web_free: 0
gslb_debug_option_http_url_mem_free_web: 0
gslb_debug_option_http_url_mem_free_url: 0
gslb_debug_option_http_status_mem_free_web: 0

Resource alloc:
gslb_debug_allocate_qname_hash_map_mem: 1
gslb_debug_dns_tcp_msg_alloc: 0
gslb_debug_gslb_controller_init_mem_alloc: 1
gslb_debug_num_gslb_controller_record_alloc: 1
gslb_debug_num_agent_init: 0
```

```
*********************************************
GSLB backend DNS debug information:
***********************************************
g_gslb_dnssec_backend_not_found                 :            0
g_gslb_dns_backend_not_found                    :        42409

*********************************************
GSLB Agent health check debug information:
***********************************************
Number of hcheck msgs sent to local controller: 51088
Number of dist hcheck msgs sent to remote controllers: 156630
Number of non-dist vip lists sent to remote controllers: 0
Number of no buf avl: 0
Number of times vip port reported down: 2012412
 Last 100 VIP ports reported by Agent as down:
************************************
VIP = 11.11.11.111, Port = 53, Reason = svr down

*********************************************
GSLB Controller health check debug information:
***********************************************
Number of dist hcheck msgs recvd: 244432
Number of non dist hcheck vip list recvd: 0
Last 100 VIP ports recvd as down:
***************************************
```

Troubleshooting IPv6 lists

The **show gslb message** command enables you to view information about IPv6 list messages sent between the GSLB ServerIron ADX (GSLB controller) and a site ServerIron ADX. The command shows both the number of messages sent from the GSLB controller to the specified ServerIron ADX and the number of messages sent from the site ServerIron ADX to the GSLB controller.

To view inform ai ton about GSLB IP list messages, run a command such as the following on the GSLB ServerIron ADX:

```
ServerIronADX 1000(config)#show gslb message 11.11.11.4
Message sent to site 11.11.11.4
        type GSLB_KEEPALIVE: 8701
        type GSLB_SET_PARAMETERS_DIST: 11
        type GSLB_VERSION_UPDATE: 8701
        type Unknown 18: 1
        type GSLB_SET_IPV6_VIP_LIST: 1
Message sent to controller 11.11.11.4
        type GSLB_REPORT: 8705
        type GSLB_KEEPALIVE: 1
        type GSLB_VERSION_UPDATE: 8705
        type GSLB_ACTIVE_BINDINGS: 8703
        type GSLB_ADDRESS_LIST_DISTRIBUTED_TS: 52227
        type GSLB_IPV6_ADDRESS_LIST_DISTRIBUTED_TS: 52227
```

Syntax: **show gslb message** *<IP_address>*

The <IP_address> parameter identifies the IP address of the site ServerIron ADX.

Debug trace for GSLB

```
debug trace feature gslb <algorithm | sticky | all | generic>
```

```
1/1 #sh debug trace summary
Count of log entries in the buffer: 2
1/1 #show debug trace
  DECIMAL   50 entries will be displayed from this starting index
  config    Show the configured debug-trace settings
  summary   Show the captured log entry count
1/1 #sh debug trace 50
Displaying 2 entries ...

GSLB Selection: Domain: ssl.brocadenet.com Client:5:1:1::100  Selected IP 16.16.
16.8 Metric:least-response

GSLB Selection: Domain: ssl.brocadenet.com Client:5:1:1::100  Selected IP 11:11:
11::25 Metric:sticky
```

Syntax: **debug track feature gslb <algorithm | sticky | generic | all>**

The optional **algorithm | sticky | all** parameter specifies the information that you want to see.

- The **algorithm** operand displays debugging for GSLB selection.
- The **sticky** operand displays debugging for GSLB sticky.
- The **generic** operand displays miscellaneous debugs.
- The **all** operand displays all GSLB debugs.

Appendix

Reference Materials

A

RFC

IPv4

IPv4 RFC 791

IPv6

IPv6 RFC 2460

DNS

The GSLB ServerIron uses the Internet Assigned Numbers Authority's (IANA's) IP address prefixes (IPv4 or IPv6) to generate an initial static database of geographic prefixes. This database consists of IP address prefixes (IP address/prefix length) and their corresponding geographic locations (such as, the continent for each IP address prefix).

IPv4

The following geographic prefixes are preconfigured:

TABLE 27 IPv4 address assignment

Address	Designation
11.0.0.0/8	NORTH AMERICA
12.0.0.0/8	NORTH AMERICA
13.0.0.0/8	NORTH AMERICA
139.20.0.0/14	EUROPE
139.24.0.0/14	EUROPE
139.28.0.0/15	EUROPE
14.0.0.0/8	NORTH AMERICA
141.0.0.0/10	EUROPE
141.64.0.0/12	EUROPE
141.80.0.0/14	EUROPE
141.84.0.0/15	EUROPE
145.224.0.0/12	EUROPE
145.240.0.0/13	EUROPE

TABLE 27 IPv4 address assignment

Address	Designation
145.248.0.0/14	EUROPE
145.252.0.0/15	EUROPE
145.254.0.0/16	EUROPE
149.202.0.0/15	EUROPE
149.204.0.0/16	EUROPE
149.206.0.0/15	EUROPE
149.208.0.0/12	EUROPE
149.224.0.0/12	EUROPE
149.240.0.0/13	EUROPE
149.248.0.0/14	EUROPE
15.0.0.0/8	NORTH AMERICA
150.254.0.0/16	EUROPE
151.13.0.0/16	EUROPE
151.14.0.0/15	EUROPE
151.16.0.0/12	EUROPE
151.3.0.0/16	EUROPE
151.32.0.0/11	EUROPE
151.4.0.0/15	EUROPE
151.64.0.0/12	EUROPE
151.80.0.0/15	EUROPE
151.82.0.0/16	EUROPE
151.91.0.0/16	EUROPE
151.92.0.0/15	EUROPE
151.95.0.0/16	EUROPE
16.0.0.0/8	NORTH AMERICA
160.216.0.0/14	EUROPE
160.220.0.0/16	EUROPE
160.44.0.0/14	EUROPE
160.48.0.0/12	EUROPE
163.156.0.0/14	EUROPE
163.160.0.0/12	EUROPE
164.0.0.0/11	EUROPE
164.128.0.0/12	EUROPE
164.32.0.0/13	EUROPE
164.40.0.0/16	EUROPE
169.208.0.0/12	ASIA

TABLE 27 IPv4 address assignment

Address	Designation
17.0.0.0/8	NORTH AMERICA
171.16.0.0/12	EUROPE
171.32.0.0/15	EUROPE
18.0.0.0/8	NORTH AMERICA
19.0.0.0/8	NORTH AMERICA
192.106.196.0/23	EUROPE
192.162.0.0/16	EUROPE
192.164.0.0/14	EUROPE
192.71.0.0/16	EUROPE
193.0.0.0/8	EUROPE
194.0.0.0/8	EUROPE
195.0.0.0/8	EUROPE
196.0.0.0/8	NORTH AMERICA
198.0.0.0/7	NORTH AMERICA
198.17.117.0/24	EUROPE
199.0.0.0/8	NORTH AMERICA
20.0.0.0/8	NORTH AMERICA
200.0.0.0/8	SOUTH AMERICA
201.0.0.0/8	SOUTH AMERICA
202.0.0.0/7	ASIA
204.0.0.0/6	NORTH AMERICA
208.0.0.0/7	NORTH AMERICA
21.0.0.0/8	NORTH AMERICA
210.0.0.0/7	ASIA
212.0.0.0/8	EUROPE
213.0.0.0/8	EUROPE
216.0.0.0/8	NORTH AMERICA
217.0.0.0/8	EUROPE
218.0.0.0/8	ASIA
22.0.0.0/8	NORTH AMERICA
24.0.0.0/8	NORTH AMERICA
24.132.0.0/14	EUROPE
24.192.0.0/14	ASIA
25.0.0.0/8	NORTH AMERICA
26.0.0.0/8	NORTH AMERICA
28.0.0.0/8	NORTH AMERICA

TABLE 27 IPv4 address assignment

Address	Designation
29.0.0.0/8	NORTH AMERICA
3.0.0.0/8	NORTH AMERICA
30.0.0.0/8	NORTH AMERICA
33.0.0.0/8	NORTH AMERICA
35.0.0.0/8	NORTH AMERICA
38.0.0.0/8	NORTH AMERICA
4.0.0.0/8	NORTH AMERICA
44.0.0.0/8	NORTH AMERICA
45.0.0.0/8	NORTH AMERICA
46.0.0.0/8	NORTH AMERICA
47.0.0.0/8	NORTH AMERICA
48.0.0.0/8	NORTH AMERICA
55.0.0.0/8	NORTH AMERICA
56.0.0.0/8	NORTH AMERICA
6.0.0.0/8	NORTH AMERICA
61.0.0.0/8	ASIA
62.0.0.0/8	ASIA
63.0.0.0/8	NORTH AMERICA
64.0.0.0/8	NORTH AMERICA
8.0.0.0/8	NORTH AMERICA
80.0.0.0/8	EUROPE
81.0.0.0/8	EUROPE
9.0.0.0/8	NORTH AMERICA

IPv6 address assignment

The initial implementation of GSLB for IPv6 addresses supports user configurable geographic prefixes as a metric in GSLB policy settings for IPv6 addresses. The default client length on the ServerIron is 64.

The following geographic prefixes are preconfigured:

TABLE 28 IANA IPv6 address assignment

Address	Designation
2001:0000::/23	IANA*
2001:0200::/23	APNIC
2001:0400::/23	ARIN
2001:0600::/23	RIPE NCC
2001:0800::/23	RIPE NCC

TABLE 28 IANA IPv6 address assignment (Continued)

Address	Designation
2001:0A00::/23	RIPE NCC
2001:0C00::/23	APNIC
2001:0E00::/23	APNIC
2001:1200::/23	LACNIC
2001:1400::/23	RIPE NCC
2001:1600::/23	RIPE NCC
2001:1800::/23	ARIN
2001:1A00::/23	RIPE NCC
2001:1C00::/23	RIPE NCC
2001:2000::/23	RIPE NCC
2001:3000::/23	RIPE NCC
2001:3800::/23	RIPE NCC
2001:4000::/23	RIPE NCC
2001:4200::/23	AfriNIC
2001:4400::/23	APNIC
2001:4600::/23	RIPE NCC
2001:4800::/23	ARIN
2001:4A00::/23	RIPE NCC
2001:4C00::/23	RIPE NCC
2001:5000::/20	RIPE NCC
2001:8000::/19	APNIC
2003:A000::/20	APNIC
2001:0000::/20	APNIC
2003:0000::/18	RIPE NCC
2400:4200::/12	APNIC
2600:0000::/12	ARIN
2610:0000::/23	ARIN
2620:0000::/23	ARIN
2800:0000:/12	LACNIC
2A00:0000::/12	RIPE NCC
2C00:0000::/12	AfriNIC